揭开网络安全的面纱，探讨网络安全的本质

增强网络安全的意识，提升网络安全的能力

网络安全

陈　震　编著

Network Security

清华大学出版社

网 络 安 全

陈　震　编著

清 华 大 学 出 版 社
北　京

内 容 简 介

无论是哪一门学科，只有研究其中的本质问题，才能在已有的基础上发展，才能在巨人的肩膀上看得更远。技术来源于生活和社会实践，对很多看似高深的理论，如果能发现它的本质、了解其产生的根源，才会对其理解得更加透彻和深入。本书编写的目的是揭开计算机网络安全的表相，探讨网络安全本质，增进网络安全意识，了解网络攻击的原理，把握攻击防范的技术，化解网络安全风险。

每个国家、组织、机构和个人都有秘密，人们都希望自己的秘密不被他人发现。而出于各种各样的原因，人们又会渴望知道别人的秘密。如果这些秘密被人获知，代价有时是无比巨大的。密码学代表了人类对机密的重视，也体现了人类高超的智慧。本书阐述了密码学在网络通信安全中的应用，同时介绍了同态加密、加密数据库、密文检索以及比特币等密码货币的应用。

本书适合作为高等院校本科生的网络安全类教材，也适合作为网络安全爱好者的参考书。

图书在版编目（CIP）数据

网络安全/陈震编著．—北京：清华大学出版社，2015

ISBN 978-7-302-39335-1

Ⅰ．①网…　Ⅱ．①陈…　Ⅲ．①计算机网络－安全技术－高等学校－教材　Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 024960 号

责任编辑：白立军
封面设计：
责任校对：白　蕾
责任印制：

出版发行：清华大学出版社

网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 装 者：
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：6.5　　**字　　数**：140 千字
版　　次：2015 年 4 月第 1 版　　**印　　次**：2015 年 4 月第 1 次印刷
印　　数：1～
定　　价：　.00 元

产品编号：063147-01

前　　言

人们享受互联网带来的便利的同时,也面临着种种安全危机。然而,或许是互联网知识欠缺,或许是过于信任开发厂家,大多数人只是将互联网作为了一种娱乐、办公、社交的便捷方式,而忽略了与联网如影随形的网络安全风险,使个人隐私与利益面临种种威胁。

当前互联网逐渐暴露出越来越多的安全问题、各种网络安全现象日益突出情况,很多研究机构都在针对互联网安全问题展开研究。然而,目前国内很少有详细介绍网络安全本质的书籍。对于热心网络安全,希望了解网络安全本质的读者,本书是很好的入门和指导书籍。

在计算机和互联网这个平台之上,许许多多的革新正在不知不觉中层出不穷地上演,人们需要及时更新自己的思维与视角,才能跟上时代的步伐。网络安全是一门交叉学科,和众多学科一样,在解决问题时有两个经典思路(学院派和产业界的区别):

① 碰到一个问题,解决一个问题——自下而上一点一点拼成系统;

② 构想系统应该是什么样子的——自上而下宏观思考构建系统。

本书有针对性地介绍了网络安全问题的产生、互联网的基本原理和设计的具体协议,以及网络安全威胁的攻击与防范等读者关心的具体问题,并针对这些问题提出了具体的解决方案。本书剖析了网络安全与密码学的关系,介绍了未来网络可能的发展方向、密码货币的诞生与发展,以及网流归档与取证在互联网安全中的重要性。

全书共分 9 章。第 1 章主要介绍安全的本质和网络的本质。第 2 章主要介绍计算机系统与计算机网络。第 3 章介绍一些网络技术和原理。第 4 章介绍网络安全涉及的内容。第 5 章介绍网络攻击的类型。第 6 章介绍网络安全防范技术。第 7 章介绍通信安全与密码学原理。第 8 章介绍未来网络技术。第 9 章介绍最近的网络安全研究的新兴领域。

书中不当之处恳请广大读者指正。

编　者

2015 年 1 月

目　　录

第 1 章　导　　论

1.1　网络安全面面观

1.1.1　不安全的世界与不安全的网络

“网络社会”(Cyber Society)是在计算机网络提供的信息通信、存储和传播的功能的信息基础设施上，由人类社会中的网民(Netizen)虚拟出来的一个社会空间，这个空间活跃的社会角色都映射到使用计算机的现实用户上。

这个虚拟的社会折射了很多现实社会的影子，反映了很多现实社会中不能获得的诉求。因此，社会的行为，如互助、竞争、攻击等；社会的关系，如伙伴、朋友、圈子等；社会的愿望，如正义、公平和稳定等，这些社会特征一样会反映到这个虚拟空间上，最后落实到提供信息基础框架的计算机软件和网络设备上。

现实社会有如下很多典型的安全事件。

(1) 2001 年的 9・11 事件，恐怖分子劫持了 2 架客机撞击美国世贸中心双子大楼，导致世贸中心夷为平地，美国社会陷入了对国家安全的担忧之中。

(2) 2008 年次贷危机，雷曼兄弟公司倒闭，美林公司破产，花旗银行大幅贬值几近崩溃，导致全球陷入经济危机，数百万人失业，经济衰退。

(3) 2009 年金融危机进一步恶化，中国和国际社会一道对美元作为储备货币所引发的经济安全问题表现出担忧。

(4) 2010 年中国北斗系统信号被破解，引发了人们对国家机密的担忧。

(5) 2013 年 6 月，斯诺登曝光了美国“棱镜计划”等网络安全计划，引发了人们对网络安全的军事竞赛担忧。

(6) 2014 年苹果手机追踪用户行踪功能被关注，引发了用户对个人隐私的担忧。

……

世界动荡不安，可以想象网络上也不会风平浪静。

1.1.2　互联网安全风险无处不在

人们平时使用手机或者计算机，主要用来浏览门户网站，收发邮件，使用网银支付，或者下载一些软件等，似乎感觉不到这里有什么安全风险。

殊不知来自网络的安全威胁从计算机连接网络的这一刻开始就已经如影随形。例如，计算机获取的 IP 地址可能是一个私有 DHCP 服务器放出来的，笔记本电脑连接的无线路由器可能是一个钓鱼的无线热点，甚至手机连接的基站也有可能是一个伪基站。

浏览器打开的网站有可能是钓鱼网站，下载的网页中隐藏各种广告和间谍软件，网页中可能嵌入了木马程序，下载的客户端软件中可能被植入了病毒，安装的新应用植入了吸费吸流量的恶意代码，收到的垃圾邮件或许就是“钓鱼”邮件等。互联网安全的风险无处不在。

1.1.3 谁控制着你的手机与计算机

人们买了一部安卓智能手机，用了段时间后发现内存不够用，想卸载一些内置应用，却发现不能卸载。如果要卸载内置应用，往往要采用 Root 方法。这就是用第三方的黑客工具取得管理员权限。但是 Root 完后，其实又把管理权托管给了提供 Root 工具的第三方。人们自始至终都没有真正的控制权。

智能手机是具有计算机功能的手机。智能手机、笔记本电脑和 PC 等这些计算机的控制权，并未完全由用户掌握。这是因为在这个场景下，普通用户是使用软件运行在计算设备的硬件平台。其中，软件开发商生产软件产品，硬件制造商生产硬件产品。

硬件制造商、软件开发商与普通用户之间作为商业产品的销售方与购买方，存在一定的责任权利的关系。用户与软件厂商之间的关系，需要有产品的使用许可证和质量保证，产品需经过测评认证，不违反知识产权。

但是，计算机系统的使用权始终不是风平浪静的，未经授权而获得计算机系统的使用权的情况始终存在。

首先，软件厂商或公司为了追求商业利益可能突破相关约定，控制引导用户的使用行为。用户是不是应该把他们的安全寄托于部分公司上，公司天然是封闭的，对用户是不负责的。无论公司对用户有多少承诺，都无法改变其盈利的最终目的，公司很可能会牺牲普通用户的利益以获得更大的商业利益。

黑客则利用系统漏洞，暴力攻击以获取计算机的使用权。恶意代码的制作者受“黑金”利益的驱动，使用木马伪装成免费安全软件，将病毒“伪装”植入某些正常软件，在用户不知情的“默许”下，获得控制权。再加上计算机司法取证的困难，普通用户的知识水平低和安全意识薄弱，使得用户在计算机控制权的博弈中始终处于不利地位。

1.1.4 谁控制着互联网

互联网作为信息发布与获取的网络平台，其控制方包括网络设备商、网络运营商和网络服务商以及其他相关的监管机构。

互联网的控制权应该掌握在谁手中呢？网络运营商、网络服务商、网络设备商、普通网络用户和监管机构之间的责权利应该如何划分？

电信网络是一个高度集中控制的通信网络，电信网络运营商同时也是网络服务商，因此普通用户对电信网络没有控制权，这种控制机制使得普通终端用户在网络应用的创新中也没有主动权。

与之相反，互联网是一个个分散多域管理的网络，通过路由器和配置路由协议，以对等或者购买服务的方式(如 Eyeball ISP)，实现不同网络之间互连互通。单个网络运

营商对网络的接入也意味着需要对其他网络承担责任(为其他网络转发流量)。基于端到端的原则,终端用户在网络应用的创新过程中拥有更多的主动权。在绝大多数情况下,网络运营商的工作就是提供一个通道,而即使是普通用户也可以自己创建网络服务提供给其他用户。

网络服务商因为直接提供用户网络服务,从用户使用其服务与产品中获得商业价值。因此,更加关心网络的通信质量,网络的连通性,以及普适的用户接入。大的有实力的网络服务商(如 Google 公司)都在纷纷自建网络,互连自建的数据中心,调优内部网络的性能,以对外提供最佳的服务。

值得指出的是,网络中性化(Network Neutrality)是目前的一个热名词。人们认为网络中性化并不意味着网络去控制化,相反网络的控制功能更需要加强,但是这种加强功能是否需要时时激活,是由网络管理策略来决定的。

1.1.5 系统的安全漏洞

当前随着计算机系统的功能越来越丰富,系统的规模越来越庞大,软硬件系统自身的健壮性由于系统的复杂性而降低,造成系统存在很多安全"漏洞",需要不断安装更新补丁修补。在软件开发过程中,开发的复杂性通过编程语言、编程类库、编译工具和操作系统调用而大大增加了安全漏洞的产生。同时,在商业化的竞争压力下,在系统的功能、性能与安全性之间的平衡中,系统开发对安全功能的重视不够,因为安全往往需要以牺牲性能为代价。

一个典型的案例是微软公司的操作系统——Windows XP 系统,它一度是最流行的桌面系统,因为对易用性的重视而忽视了安全性,导致大量安全问题的产生;而 Windows Vista 系统,由于过于重视安全性而导致性能的下降,大大减少了用户的接受程度,成为昙花一现的短命产品。

1.1.6 网络空间

赛佰空间(Cyberspace)是由互联网连接的信息系统组成的信息空间,与目前现实四维空间对应。这个信息空间包括虚拟的社区、个体与文化,计算机网络系统是该信息空间的支撑。

计算机网络系统本身就是大规模的分布式系统,需要解决可靠性、高效率和低成本的问题。信息以网包为载体,通过网络系统传递。计算机网络产业是一个繁荣的生态系统(Ecosystem),网络系统也是一个基于计算机系统的基础设施,其每个组件都是计算机系统。由组件构造新的组件,最后组成服务产品,符合人类不断建造更大可用系统的内在动力。

1.1.7 网络安全是什么

互联网安全是赛佰空间中互联网连接的信息系统的控制权的博弈。互联网作为信息通信的基础设施,功能类似一个国家的"神经系统"。控制了互联网上的信息导向,就

可以做到舆论导引等。

什么是网络安全？从技术层面来看，网络安全是一种博弈。计算机系统和计算机网络范围内，研究基于网络的系统攻击原理及技术，研究基于网络的保护方法和抵抗可能的破坏及风险。

从国家层面来看，大国都在角力基于互联网的赛佰空间控制权，进行防御与进攻。平时进行情报收集和信息渗透；战时则进行渗透控制和框架破坏以及摧毁性打击。如美国斯诺登案暴露的网络监控案例。

从商业层面来看，控制用户的网络行为，就可以获得更多的商业价值。无论是安全软件的行为，还是黑客的背后淘金行为，或者是网络黑社会的敲诈勒索行为，抑或是恶意商业竞争之间的互相攻击和防御，都使得网络安全市场面临军备竞赛的局面。

从人的层面来看，网络安全的根源是人。人性存在“善”与“恶”，人的行为与环境互为影响，人的行为充满了叛逆、对抗、好奇、热心等。

开放的网络接入环境和开放的网络服务，使得做坏事成本降低。再加上审计缺失与隐私功能，使得网络取证难，而较难被追查。在网络环境下，每个人都犹如戴了一副面具，消除了顾虑，带来了更大的自由度，形成了网络环境对于人性的“善恶”的放大效应。同时也造成了网络复杂而难以管理的环境，除了需要国家来立法、采取强制性的管理以外，更需要每个人的自觉，以营造良好的网络环境。

1.1.8　互联网的环境与文化

互联网的技术标准主要由 IETF 制定，这些标准可以公开评阅和发布。IETF 是一个自发的松散组织，它为互联网技术的工程和演变做出了重大贡献。IETF 是参与制定新互联网标准规范的主要机构。IETF 的文化传统之一体现于 David Clark 早期说的有关 IETF 的一句话：“我们拒绝国王、总统和投票。我们信奉‘大致共识’和‘运行的代码’。”IETF 内普遍接受的另一个信念则如 Jon Postel 早期所说：“发送建议时要保守，接受建议时要开放。”

互联网工程技术也是人类的文化结晶。互联网的工程技术体现了人类社会的意识形态，是集中式更有效，还是分布式更合理？云计算代表前者的集中主义形态，P2P 对等网络代表后者的自由主义形态。

互联网架构是分布式更可靠，还是集中式更安全可控？从过去高度控制的电信网络，发展到分布式自治的互联网。未来的发展是回归高度可控，还是走向更加分散管理？根据不同的设计理念，演化出了不同的未来网络形态，如软件定义网络（SDN，由统一的控制器负责网络的资源管理）和信息中心网络（ICN，以信息交换为本质的分布式网络）。

覆盖网络是当前互联网上的一种重叠组织，覆盖网络的发展，是在现有网络的基础上，构建一个又一个的虚拟网络。这些虚拟网络，可以认为是一个个虚拟社区（Vartual Community），也代表着不同的价值取向和思想形态。从内容的共享到比特币挖矿，凝聚每个社区的是动机和激励；从 BitTorrent 网络的帕累托效率（Pareto Efficiency）到比特币网络的交易等，保障了虚拟网络系统的稳定。哪里有动机与激励，哪里就有虚拟社

区的发展空间。

1.1.9 霍布斯哲学的解释

托马斯·霍布斯(Thomas Hobbes)是英国的著名政治哲学家,他创立了机械唯物主义的完整体系。1651 年,霍布斯出版的《利维坦》详细描述了人类从"自然状态"如何形成"利维坦"以及国家。

霍布斯描述的"自然状态",是指每个人都需要世界上的每样东西,也就有对每样东西的拥有权力。但由于世界上的东西都是不足的,资源总是受限的,所以这种资源权力的争夺导致"人和人的冲突"便永远不会结束。而在"自然状态"下,有一些人天生或者后天可能比别人更聪明或更有力量,但没有一个人不怕被暴力攻击而丧命。当受到这些威胁时,人必然会尽一切所能来保护自己。因此,霍布斯认为保护自己免于暴力攻击就是人类最高的需要,而权力的产生就是来自于这种需要。

但是,暴力冲突并不是对所有人都是最有利的。霍布斯认为为了考虑自身安全和避免被他人侵犯,只有在社会契约(Social Contract)的约束下,社会才能有和平。因此,霍布斯认为社会是一群人服从于一个威权,而每个个人(Individual)将自然权力交付给这威权,让它来维持内部的和平并抵抗外来的敌人。这个威权就是一个强而有威信的"利维坦",只有它才能令社会契约实行。

1.1.10 互联网的"利维坦"

因为互联网没有一个单一的控制权威,并且是开放接入和获取服务,技术的创新层出不穷,监管往往赶不上创新的步伐。因此,互联网的生态可以认为是一种霍布斯所说的自然状态。

如同"霍布斯主义"(Hobbesian)描述的每个个体是自私而野蛮地进行一种无限制的竞争情况。而少数个体比其他个体了解更多的技术,比如黑客、安全公司等,从而可以获得比其他个体更多的能力,就形成了"利维坦"。这些个体就容易攻击、控制别的机器。其他个体只能依附在某些"利维坦"之下,依托利维坦提供服务和保护,如各种杀毒软件公司等。

用户与"利维坦"之间签订的不仅仅是产品或者服务的合同,或仅仅是托管了自己的网络账户或者文件数据,以获取网络使用的便捷和安全;这种托管和信任更是心理上的合同,以信任互联网公司的其他产品或者服务。

1.2 安全的本质

要想了解网络安全,从身边的社会中可以看到同样的影子。

1.2.1 安全的定义

安全一直和威胁相随相伴。自人有自我意识以来,便能够区别自我和非我,外在的

世界一直有危险和伤害。自然环境并非总是友好的，来自外界的各种攻击不断，威胁着身心。正如老子所言："天地不仁，以万物为刍狗。"

安全(Security)的字面意思是免于风险和伤害。安全就是用来摆脱威胁和伤害。

本质上"安全"是一组物质设施、一种社会精神意识和个体的心里感觉。人的安全感来自什么？衣食无忧，家庭幸福，周围环境受我控制，职业和社会状况可确定可控。社会安全感来自什么？犯罪率低，社会稳定，公民都有好的社会保障体系和福利体系。国家安全感来自什么？民富国强，拥有最先进的武力等。

1.2.2 如何保障安全

为了保障安全，在人类社会中如何做到呢？

(1) 了解威胁和风险。对威胁进行防范，要"未雨绸缪"，时时监控；对攻击进行阻挡，要"防御性进攻"。

(2) 提高自身的对抗能力。通过打疫苗，提高免疫能力，对危机的反应能力，对危机的控制能力。

(3) 隔离是保护安全的直接手段。如防盗门锁、禁闭室、监狱、黑名单、经济封锁和制裁等。

(4) 增强对威胁的控制性(防御走向进攻)。知己知彼，分析自身的脆弱性和黑客攻击方法和手段，主动防御(Proactive)。

(5) 惩罚手段。经济处罚，限制人身自由，以暴制暴等惩罚手段。

1.2.3 "适度"安全

绝对安全状况是不存在的，因此对安全的追求是一种无止境的追求，是一个永无止境的过程。安全的需求，基于人的现实需求，满足现实需求，基于人的心理需求，满足心理需求，才会有相对的安全感。

对于安全，可以引入风险控制模型，如图 1.1 所示。举个例子，某些地区晚上出门是很危险的，要保障安全，晚上就尽量不要出门，以避免被人打劫；实在要出门，带个防身工具，如棒球棍，也可以减缓被人打劫的风险；最好几个人一起出门，可以在被人打劫的时候转移风险；最后依然有风险，但觉得风险可控，就出门吧。

因为安全产品对应的风险并不一定发生，这和买商业保险是一样的。因此，制造不安全气氛，到处发布各种安全事件损失以兜售安全产品的现象也会经常发生，这就是"安全"讹诈问题。安全资源的过度配置可能导致"过度"安全，为了保护 1000 元的资产，却需要花 10 000 元的安全产品投资，这是不合理的。分段对风险的评估是配置安全资源的依据，但也要避免因小失大的问题。但是对涉及国家安全的机密数据和文档，其价值是不能用经济利益来衡量的。另外，人是整个安全保障体系中最重要的环节，因此即使进行了安全投资，也要在管理等其他人为因素上多下工夫，确保排除人为因素带来的安全隐患。

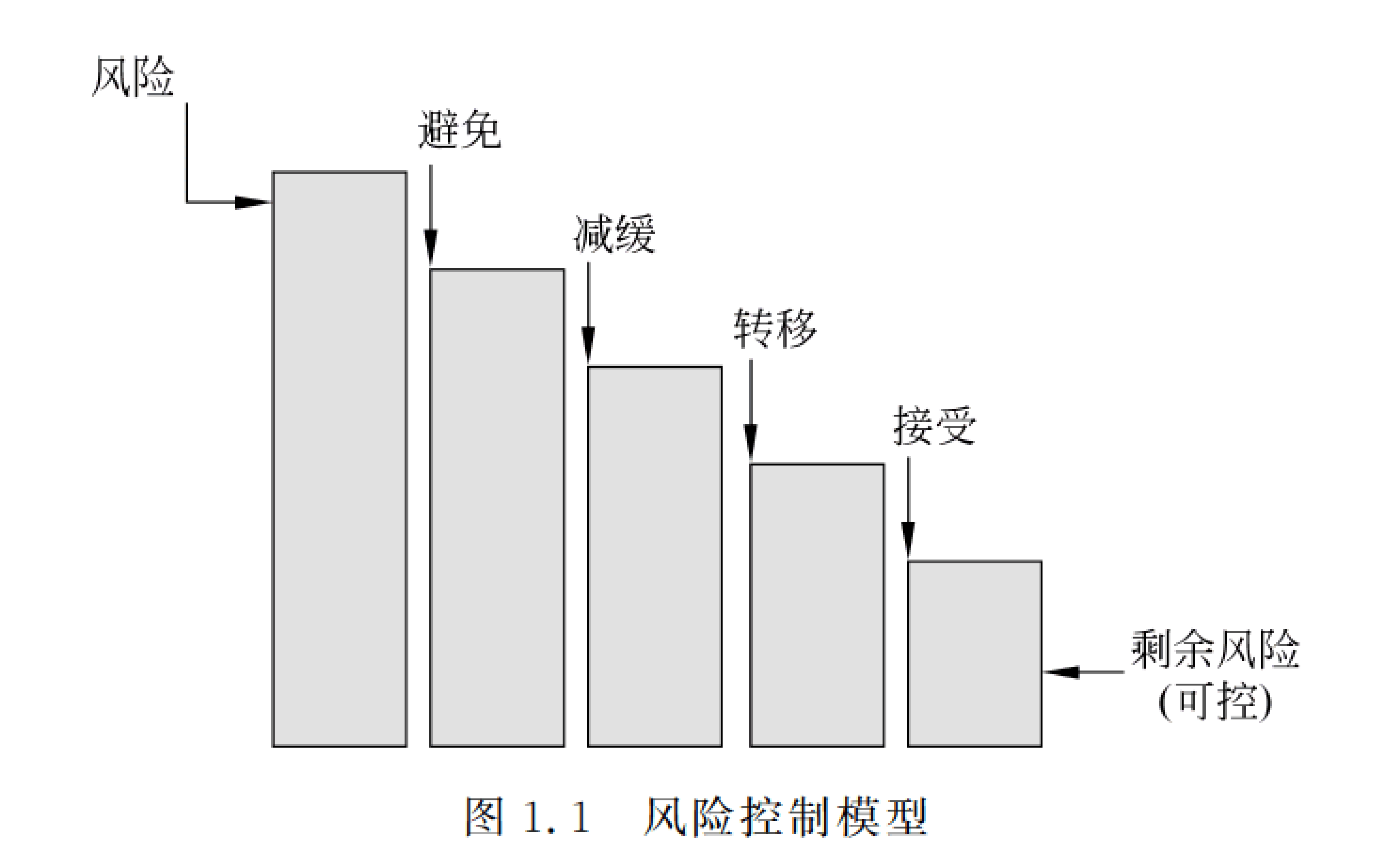


图 1.1　风险控制模型

1.3　网络的本质

1.3.1　网络的定义

任何多个相关的个体都可连成网络，网络(Network)是被联网(Networking)的结果。哲学讲万事万物都是有联系的，是因为任何事物都不会无缘无故产生、发展和消亡，总是处于联系之中。这个联系就是网络。

个体可以小到原子，大到社会组织、宇宙天体。每个网络都有其特定的功能。基因调节网、神经网络、大脑网络、新陈代谢网络、知识表述语义网、电网、交通网、物流运输网、经济网络、社会网络等，这些网络可以处理、存储、传递和接收能量、物质等广义的信息。网络是群体结构，其实，任何事情的发展都是网络的或者说是社会的。几乎没有单独的不受任何影响，也不影响任何其他个体的独立事件，所有事件必是某网络中的一个事件。

大规模的网络系统一直是大自然的奇迹，更是人类的伟大发明。

宽广的长江流域，在重力与地貌影响下，小河汇聚成支流，支流汇聚成主干，最后形成大江，奔向大海大洋，蔚为壮观。

纵横交错的灌溉网络，是劳动人民的智慧，将水资源运输、供给、调配到不同的地方，浇灌了农作物，生产了所需的农产品，养育了各族人民。

雄伟的长城，最初是秦朝将战国时代各国分散的、各自修建的城墙连接起来，形成的统一的连通的工程，借以统一部署，快速调动防御力量，抵御外族入侵。

庞大的高速铁路与高速公路，四通八达，纵贯东西南北，穿隧道，过大江，形成快捷的国家交通网络。

便利的地铁网络，在地下修建，穿沟走壑，可以从一地，转乘到达另外地点，形成快捷的城市交通网络。

1.3.2 网络的意义

大自然的网络化系统和人造的网络化系统，其推动力和目标是不同的。人造网络系统扩张的原动力更在于人的欲求，能获得更多的资源，更大的能力。

网络系统扩张的外在推动力来自于竞争。优胜劣汰一直是大自然和人类社会的基本法则。社会是由人组织而成的，组织方式与个体的差异，以及组织的目标与使命有很大的关系。

资源总是有限的，系统扩张或抗衡别的系统扩张，都需要竞争资源，增强能力。将所占领的资源并入其中，吸纳新的能力。

单个组织及个人的资源和能力也是有限的，往往在竞争中处于劣势。需要互相之间共享资源，互相之间补充能力。

联网，将分散资源或者系统连接起来，达到系统资源聚集，增强能力，是系统扩张、竞争资源的基本方式。

1.3.3 通信网络

通信网络是传递信息内容的网络。作为人类语音通信的电话网络早就存在（自 Alexandra Graham Bell 发明电话始，有 100 多年的历史），其他如电报网络也有很长的历史。3G 和 4G 无线网络的兴起，将无线数据通信进一步发展到普适的地步，传统通信网络运营商为互联网接入提供丰富带宽以后，这些运营商在提供通道的同时，目前也在大力开发内容，以提高网络的“黏性”。

1.4 计算机网络的本质

1.4.1 网络的本质与功能

传统的通信网络负责信息传输和交换，通信网络运营商主要是作为信息的通道商，收取交通费用，并不提供内容，如电信网络、X.25 数据网络等。从 1946 年电子计算机的出现，将计算机系统连接起来的共享计算/存储等资源的需求，是计算机网络产生的直接原因。另外，通信网络也转为全数字化并计算机自动控制。

计算机通过计算机网络来完成信息的交换。计算机网络由路由器和通信链路组成。计算机网络通过网络设备将独立异构的计算机系统连接起来，完成计算机系统之间的资源共享。计算机网络要解决的一个核心问题是需要定义一套原语（Primitive），即通信协议（如当前互联网采用的 TCP/IP），让不同的异构计算机之间能够交换数据。此外，计算机网络要研究如何有效地连接计算机系统，因此需要光通信等通信技术作为基础。通信技术的革命为计算机网络的普及打下了基础。

这种网络的节点是计算机，边是传输层或应用层的各种连接。从信息的角度看，计算机网络完成信息的各种传递。计算机和人的最大不同是计算机没有自我意识，因此

信息对计算机的影响并不改变计算机的行为目的，虽然计算机可以协作和分工完成一些事情，也可以学习，但仍然是机械的，而不是具有自我意识的。

计算机网络的典型例子有 Internet、P2P、CDN 等，它们是全互联的或全连通的。为了完成各种信息处理任务，计算机网络也许把信息传递的任务交给通信网络来完成，也就是说通信网络可以为计算机网络提供信息传递服务。但计算机网络完成的任务和通信网络是没有关系的，它可以基于各种通信网络，比如 IP 网、电话网等。只是在考虑效率时，才考虑下层通信网络。

随着通信技术的突飞猛进，信息通信的通道价值日益降低，而通信内容的价值比较高。互联网最吸引人的是 Web 内容和各种音视频等，互联网提供了丰富的内容，逐渐取代了一些传统的媒体形态，因此互联网已不再单纯是作为网络存在，而是作为一种新的内容发布与获取的场所而存在。

除了狭义的信息网络外，还有广义的信息网络，如计算机网络是用来获取和发表信息的工具。目前互联网是基于端到端原则，计算与通信还是基本分离的，图 1.2 给出了实际的互联网结构图。由互联网运营商将各局域网与终端接入骨干网(Backbone)。

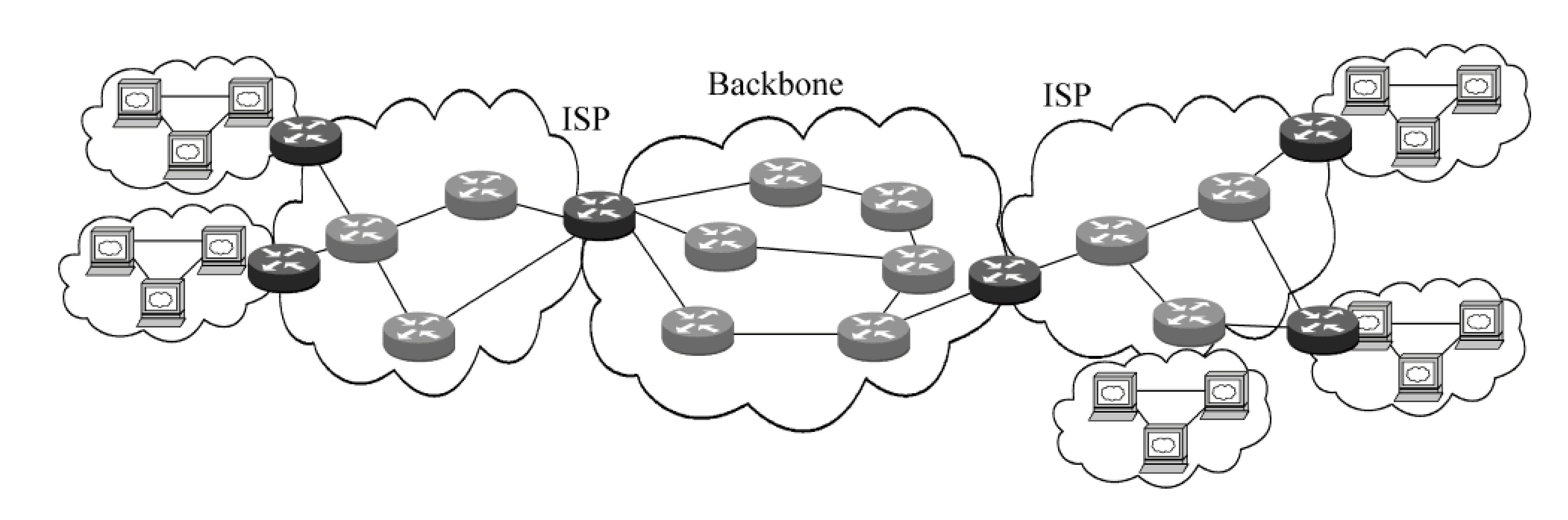


图 1.2　实际的互联网结构图

计算机及其信息网络始终是人的代理、人的工具，开始帮助人处理信息、传递信息、存储信息、发布和获取信息。当前网络中的每一个事件都基于个体目的，比如我要信息(内容获取)，我们要发布信息(内容发布)，我要通信，我要处理(服务)等。包括 CDN 也是为个体服务的。但是，从更高层面看，无数个体在达到自己利益目标的同时，其实也是在帮助别人，回馈社会，这一点非常类似经济学知识，因此有网络经济学这门学科。

1.4.2　网络设计

设计 P2P 网络系统的人，并不想让计算机网络控制在某些人手中，转发权的垄断意味着没有竞争。P2P 思想，人人皆有转发权是网络创新的根本。

现有的 Internet、电话网以及正在兴起的信息中心网络，都是为满足人们的某些需求而设计的，而不是根据网络本身的自然原理设计的。目前尚没有网络应该是什么样的理论。因此网络的设计取决于基本需求的确定和设计原则的确定。

观察历史上的通信网络，其演化的动力始终是人们的需求。比如会话的需求、抗核打击的需求、内容发布与检索和存取的需求(如 HTTP、Search Engine、Web、P2P、

CDN、CCN 等）。CCN 现在想重新设计互联网，所以应该重新深入考虑人们或社会对通信网络的基本需求。比如 IP 网的基本服务是传递信息，CCN 的基本服务可以说是“传播”信息。那么到底哪个是更基本的需求呢？IP 的信息传播服务是建立在信息传递的基础上（即信息的散播要在应用层实现），因为 IP 网本身是一个信息传递网络；而信息中心网络的传递服务要建立在传播的基础上（即点对点通信要高层参与），因为信息中心网络本身是一个信息传播网络。

如果能确定人们对通信网络的基本需求，也就确定了通信网络的基本功能，这方面，IP 做的是相当不错的，IP 只是完成一个基本功能，其他任务放在应用层去实现，这是符合端到端原则的。

因为人性基本需求不变，所以如果能正确判断人们对通信网络的基本需求，就可以设计一个基本功能不会被革命的网络或者是内在可演化的网络，就像冯·诺依曼结构，即使是发展成了云计算，也没有改变这种结构。因为不变的东西（如需求、思维逻辑）可以由不同的技术满足，技术可以万变，可以革命，可以变得越来越合理。

确定了人们对通信网络的基本需求，即确定了通信网络设计的基本目标。然后是确定一些基本的设计原则，比如标准化原则，网络的协议应该是标准化，无关种群/国家和文化，这样才能建立起人与信息的互联；端到端原则，通信网络完成基本功能，其他功能最好放在上层设计。

最后也可以考虑到底需不需要单独的通信网络？即单独的信息的传播或传递层，而不管信息的处理和存储。

第 2 章　计算机系统与计算机网络

2.1　计算机系统

与计算本质相关的数学理论是计算理论，它主要研究计算机能做什么（计算的可行性），需要多大的时间和空间开销（计算复杂性），如何解决某些特定问题的过程与步骤（算法），如何为速度、空间或者能耗等进行调优（最优化）。

计算机系统由硬件（Hardware）系统和软件（Software）系统组成，根据不同的应用场合，计算机系统的硬件和软件配置将会有很大的差异，计算机系统形态分为 4 种。

（1）嵌入式计算机：智能手机、平板（Pad）、工控设备、家电控制器等。

（2）个人计算机：PC、笔记本等。

（3）中型计算机：服务器（文件、图像处理、金融交易等）。

（4）超级计算机：网格、数据中心等。

实现计算功能的计算机系统，包括人机接口、输入输出系统、存储系统和处理器单元等。计算机系统首先是一个人造系统。从工程学的角度，计算机系统架构和其他建筑工程没有本质的区别，都是采用基本组件按照系统结构进行搭建，将尽量地复用已有的功能组件，减小成本。在系统架构的过程中，为了克服创建大系统的复杂性问题，都会进行等级化、组件化，便于使用工具、分工协作等。因此计算机系统带有演进性、缺陷性等人类社会的特征。

计算机系统的发展也体现了人类在技术上不断追求更大、更快、更强的精益求精精神。计算机系统也在不断演进，不断满足计算的新需求。

2.1.1　个人计算机

1. 个人计算机硬件

计算机硬件（Hardware）是通过电子线路板（PCB）集成的一组集成电子器件和分立电子器件。计算机硬件具有明显的组织结构（如处理器/存储/显示/连接）。处理器有 Intel Core 2（酷睿）和 Xeon 系列（至强）、AMD FX 和皓龙系列等，存储器有高速缓存（Cache）、内存（Memory）、闪存（Flash Memory）、固态盘（SSD）和磁盘存储器（Disk），外部 I/O 接口设备包括 USB、鼠标、键盘、显示接口、音视频接口等。与计算机硬件相关的学科有微电子物理、材料学、电磁学等。

计算机硬件体系结构设计是一门艺术，与人类社会结构相一致，其特征也包括人造系统的所有特征（等级化、组件化、经济性、演进性、缺陷性等）。

常用 PC 主板架构(CPU 前端总线＋北桥＋南桥)(Intel Core Duo 或 Core 2)如图 2.1 所示。其中CPU 要访问闪存,需要 MCH 统一协调。

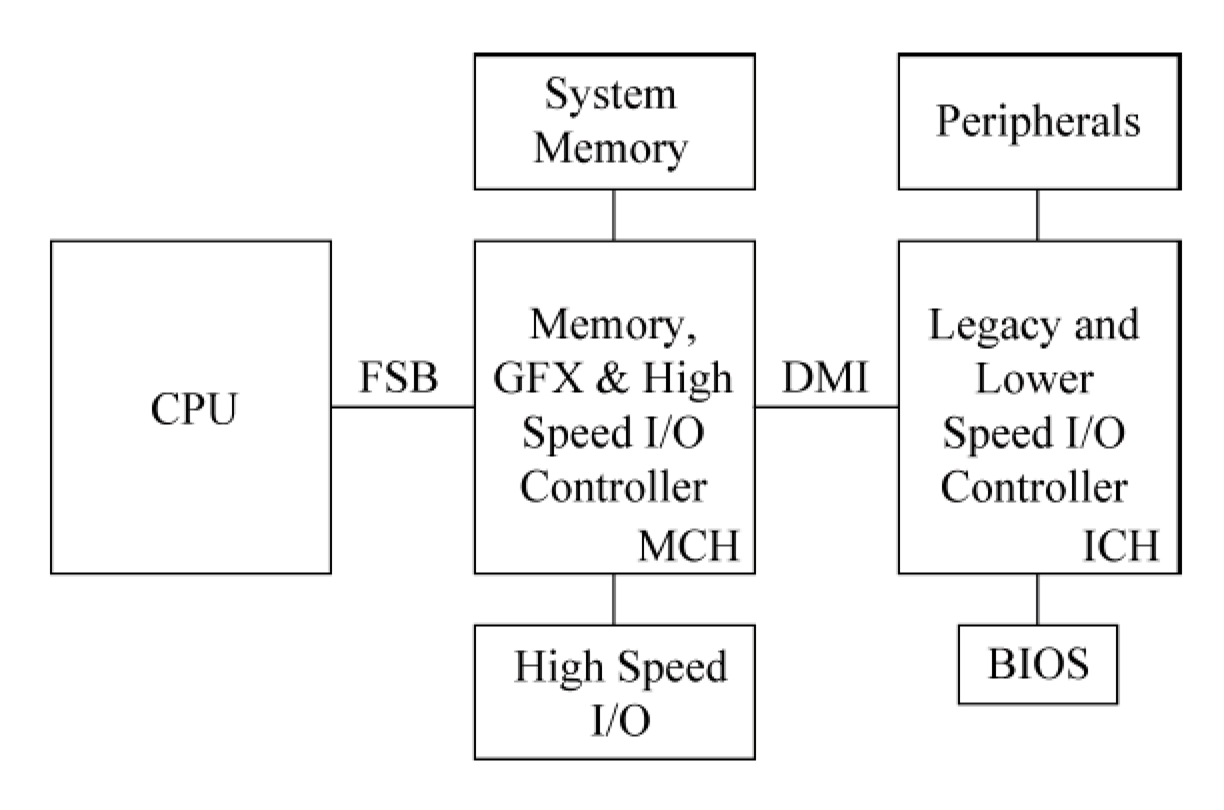


图 2.1　PC 主板架构

新一代设计把前端总线 FSB 改为直接高速连接 QPI 架构(Intel i7 处理器)如图 2.2 所示,这样设计的明显优点是 CPU 访问内存不存在冲突,效率更高了。

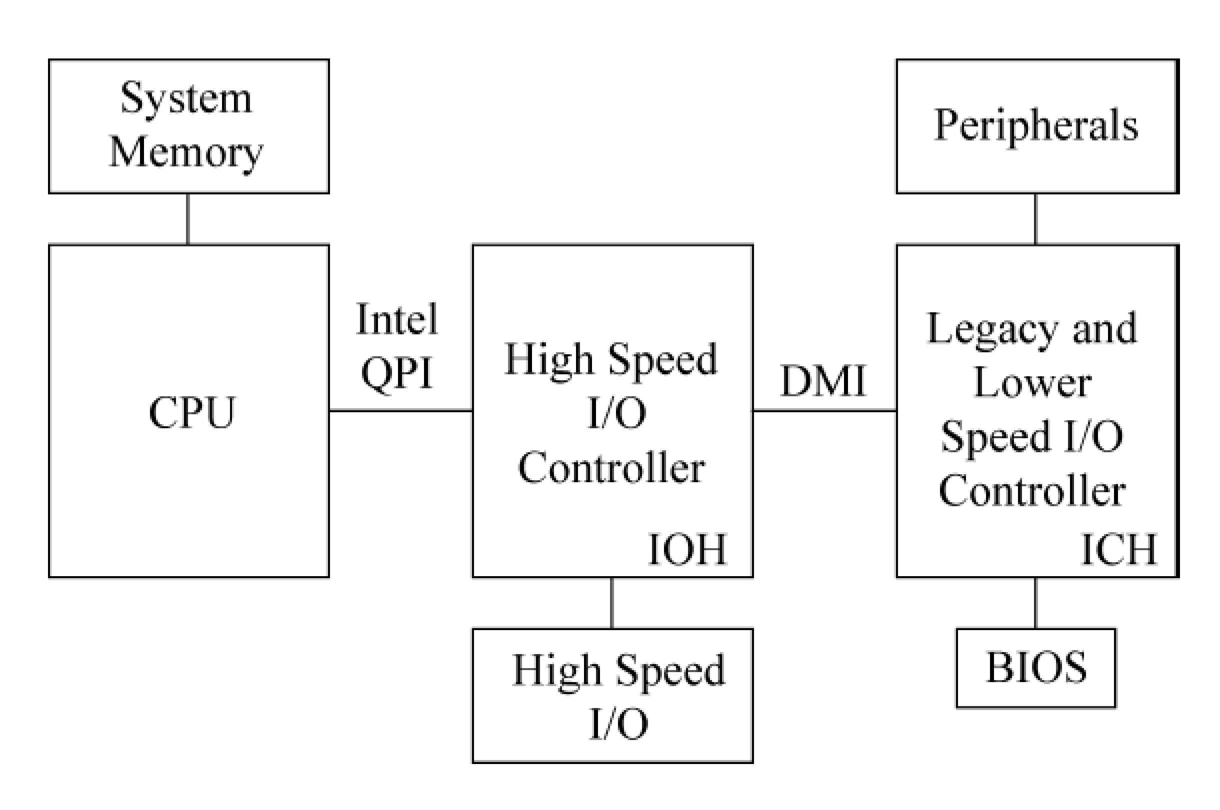


图 2.2　PC 主板直接高速互连

除了主板设计外,处理器内部设计也在不断演进,一款 32 核处理器结构如图 2.3 所示。图中每个硬件 Core 上,设计了 4 个逻辑处理器,这样设计可以并行同时处理更多任务。

2. 个人计算机软件

怎样生成计算机软件?软件生产是一个软件工程涉及的领域,需要程序员们协同编程(Programming)。一般来说,计算机软件是采用计算机工具软件制作出来的。对于软件要完成的功用,先用计算机程序语言(汇编语言、C、C++、Java、C#、Python、JavaScript 等)编写出来,调用计算机程序类库 API 和 OS 调用,采用编译器(如 GNU、VC、Intel、SGI)等生成不同平台上可执行的代码。

软件设计需要软件架构,尤其是操作系统(Operating System)和应用程序(Application Software),划分组件和功能、进程和线程。

软件又分为以下两种形态。

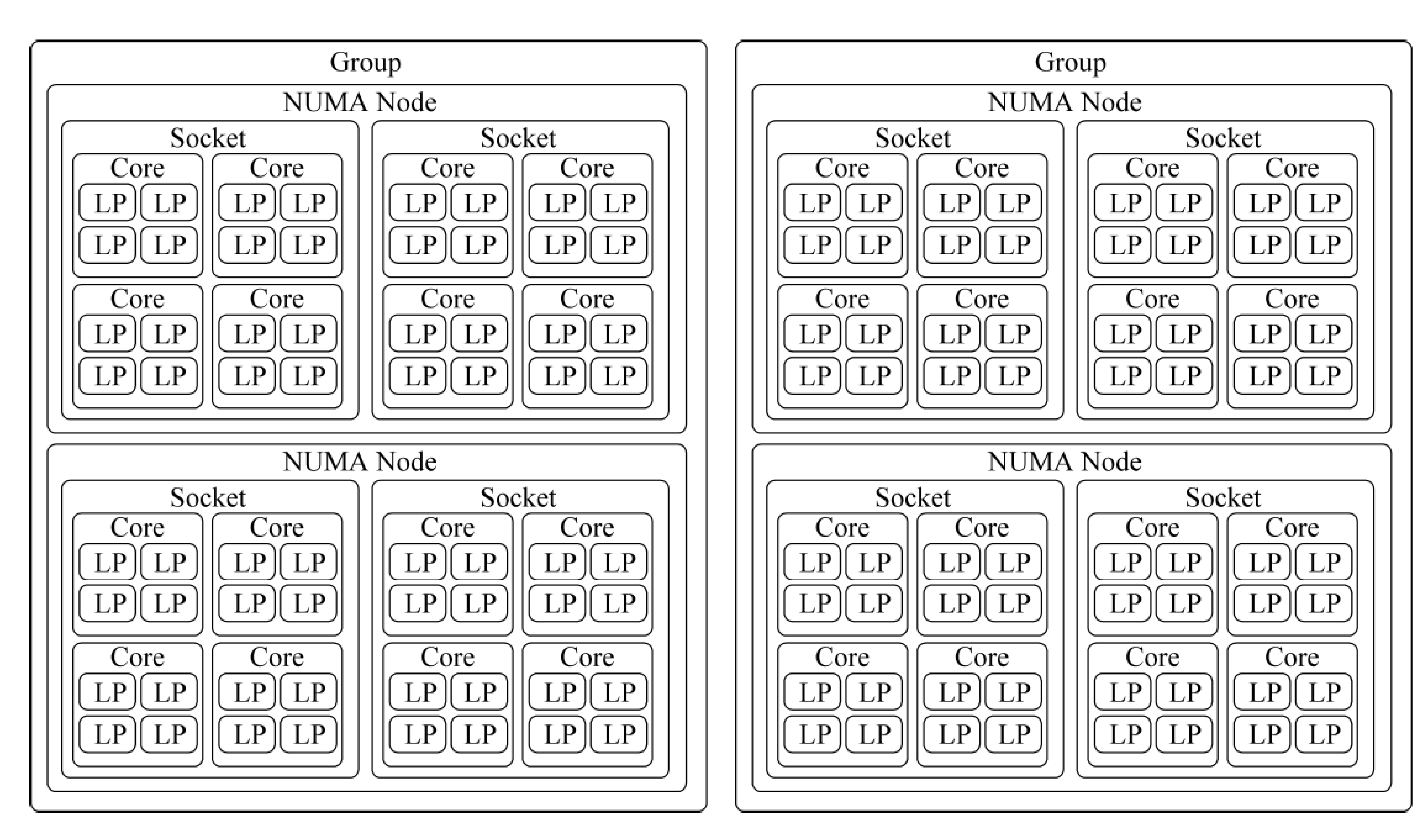


图 2.3　32 核(128 线程)处理器

(1) 系统类软件：操作系统、数据库等。

(2) 应用类软件：桌面办公软件，手机 APP 应用等。

目前基于 Web 的应用越来越流行，富客户端(RIA)的应用使得传统 C/S 结构出现了对等的趋势，相当部分的计算任务会转移到本地机器来实现。很多以前的软件都可以在 Web 浏览器中运行。

比较引人注目的是 Google 公司的 Native Client 技术使得在 Chrome 浏览器中运行二进制代码几乎和在本机上运行的软件一样快，这样就大大削弱了 Microsoft 公司的 Windows 系统在传统桌面软件方面的优势地位，图 2.4 给出了 Windows XP 系统的结构，图 2.5 为 Windows 7 和 Windows Server 2008 的内核结构。

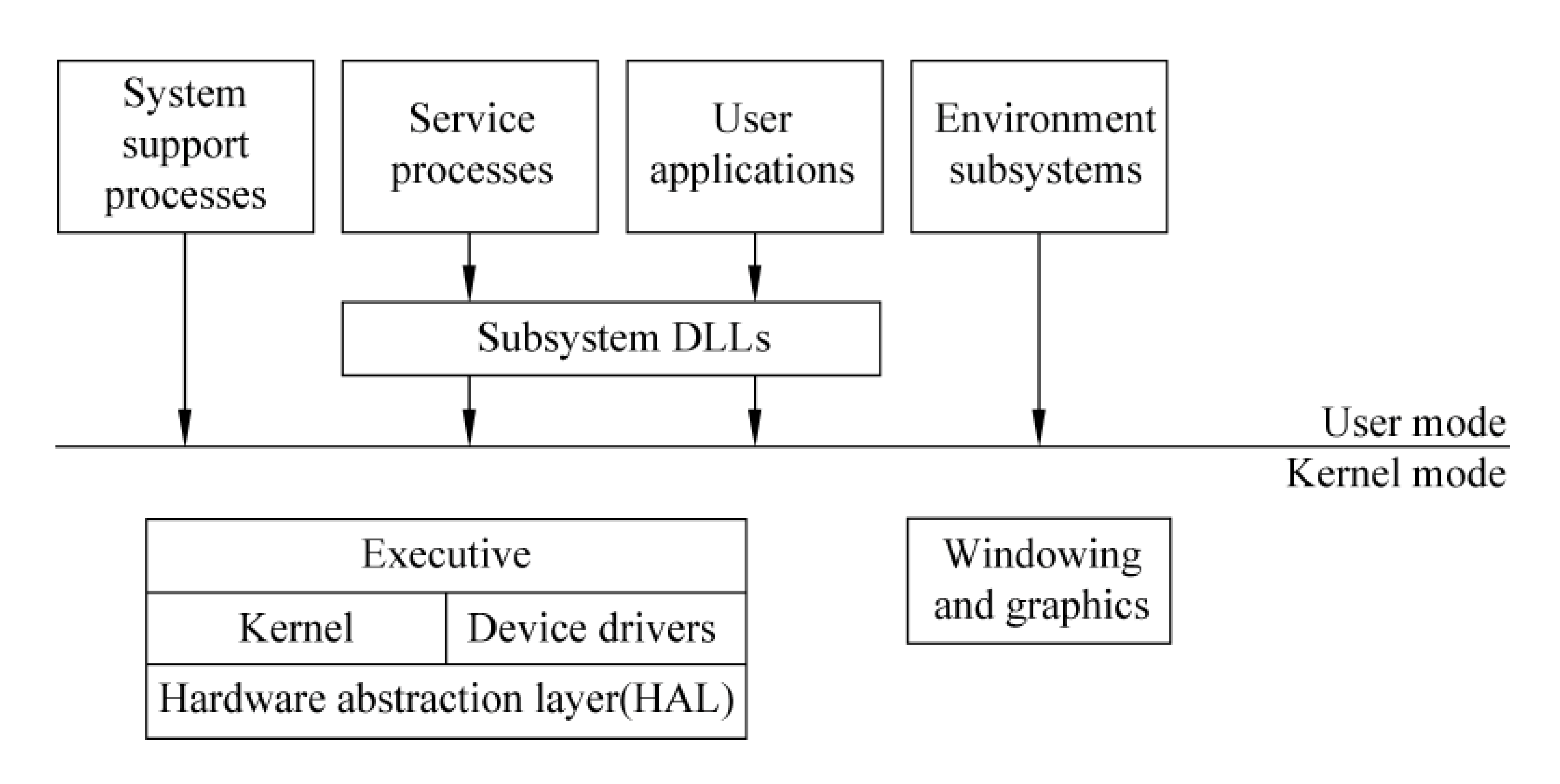


图 2.4　Windows XP 的系统结构

Google 公司开放的 Android 系统，本身基于开源的 Linux 系统，具有功耗低、功能丰富等特点，因而在手机、平板电脑等嵌入式设备上应用显著。

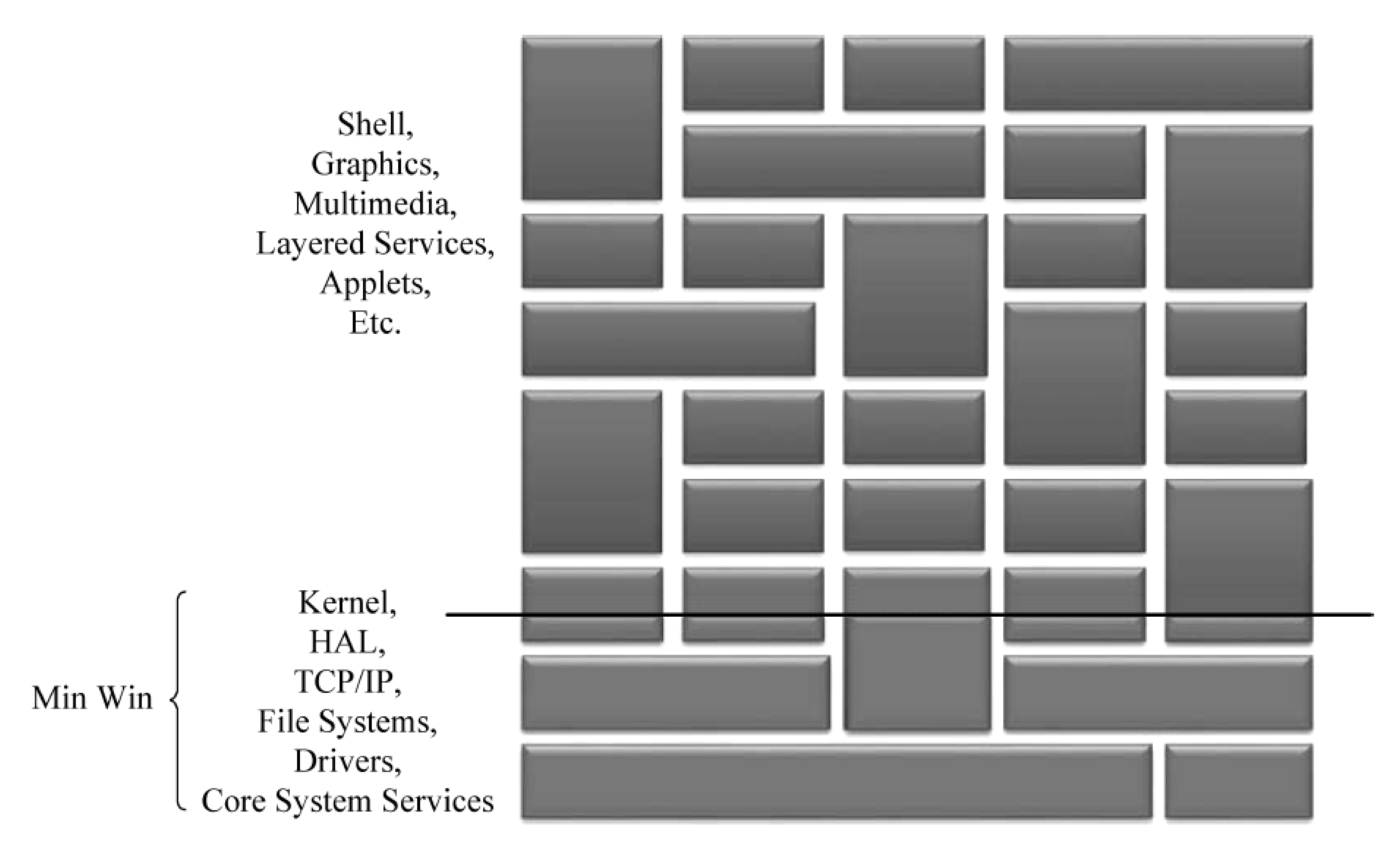


图 2.5　Windows 7 和 Windows Server 2008 的内核结构

软件体系结构设计是一种艺术，目前不同的操作系统（如 Berkeley FreeBSD、Windows、Ubuntu Linux 等）其系统架构也有很大差异。因此计算机软件的特征也包括人造系统的社会特性，如等级化、组件化、演进性、缺陷性等，Linux 系统结构如图 2.6 所示。

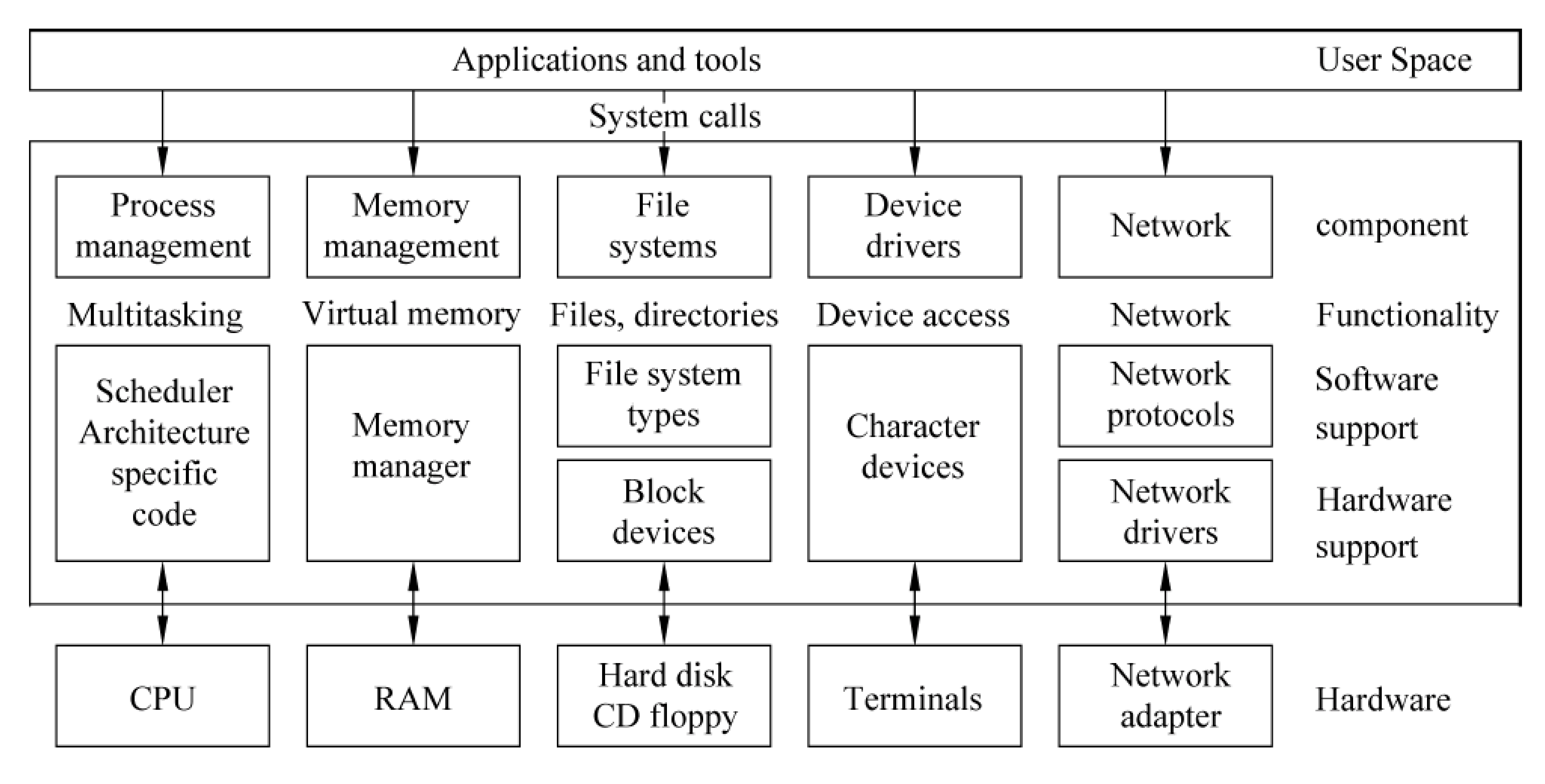


图 2.6　Linux 系统结构

2.1.2　移动智能终端

以 Android/iPhone 为代表的移动智能终端和穿戴式的设备，引领了新的计算革命浪潮，如智能手机、谷歌眼镜、集 Wi-Fi 等联网功能服装、智能手环等。

随着移动设备终端的快速发展，iPhone 处理器从 32 位架构进化到当前 iPhone 5S 版本的 64 位架构，仅用了 6 年的时间（2007—2013）。而在桌面计算上，Intel 处理器从 32 位到 64 位到的发展整整持续了 20 年（1985—2004）。手机的存储容量也随着存储

设备的价格降低而不断增加。智能移动设备演进大大加速。

智能手机的用户日益增多,而其中大部分功能是由第三方应提供。第三方应用经用户的允许,就可以访问隐私数据(如电话号码、SIM 卡号码等),其用户隐私数据保护可信性值得人们关注。

在这些应用程序中很多都是将远程云服务器的数据与本地感应信息结合来提供,比如 GPS 接收器、照相机、麦克风和加速器等。这些应用程序通常对于访问隐私的敏感数据有着合法理由,但是用户同样也希望他们的数据被恰当使用。然而开发者对采集的用户数据的滥用,和本地传感器采集用户数据所带来的隐私风险就是使用第三方程序会带来危险的最好例证。

2.1.3 云计算和大数据平台

1. 虚拟化技术

虚拟化技术就是在一台物理服务器上虚拟出多台虚拟计算机,这些虚拟计算机都有自己的操作系统,可以分别执行自己的任务,就像在真实的计算机上一样。由于现在物理服务器的资源在较长时间内都处于空闲状态,如果通过虚拟化技术整合出多台虚拟机供不同用户使用,就大大提高了资源利用率。

除此之外,虚拟机可以在物理服务器之间自由迁移,当一台物理服务器资源不足时,人们可以将虚拟机迁移到其他空闲的物理服务器上,实现灵活资源调度。最重要的是,虚拟技术的使用节约了采购、维护硬件的成本,虚拟机可以实现快速部署和备份,很轻松地搭建网络平台。

2. 云计算

近年来,随着互联网技术、虚拟化技术的进步,云计算技术飞速发展,在工业界也得到了广泛应用。云计算是指通过网络以按需、易扩展的方式获得所需服务,使得计算资源(包括服务器资源、存储器资源、应用软件资源等)可以通过互联网进行传输,成为像水、电一样的商品,既取用方便又价格低廉。这种服务可以是提供硬件资源、软件资源、互联网资源,也可是其他服务。它意味着计算能力也可作为一种商品通过互联网进行流通。

越来越多的互联网公司开始组建自己的数据中心,将上万台计算机甚至几十万台计算机连接成一个云计算平台,通过云计算平台可以实现很多以前不敢想象的超大规模分布式计算。

主要的云计算平台有 VMware 虚拟化技术构建云计算平台 vSphere,可以搭建由 vCenter 集中管控的私有云平台。开源的 OpenStack 和 Apache CloudStack 云平台管理软件都可以搭建实用化的云计算平台。

3. 分布式系统

单台计算设备总是有计算和存储的容量问题,为了能够解决超大规模的计算和存

储问题，可以把成千上万台机器整合起来。一个需要非常巨大的计算能力才能解决的问题，可以分成许多小的部分，然后把这些部分分配给许多计算机进行处理，最后把这些计算结果综合起来得到最终的结果。

为了给普通用户提供超大规模计算和存储服务，可以把用户的计算和存储请求进行适当分解，之后通过网络将它们传输到各个服务器上进行处理，最后再将结果整合起来发还给用户，这样能够大大缩短用户的等待时间，也最大化地利用了本地的计算资源。

像谷歌、百度等互联网公司就是采用这些分布式系统技术，爬取、索引和排序全球的网页，使之为用户提供搜索引擎服务。分布式系统技术要解决服务器的故障，数据一致性，以及高性能的计算问题。2013 年 ACM 图灵奖颁发给了微软研究院的莱斯利·兰伯特(Leslie Lamport)，以表彰他在分布式系统中的贡献。

4. 大数据隐私

正如冯象在《政法笔记》中描述的那样："隐私是人类文明的一个标志。事实上，将个人的身体、事情之一部划归'私'的范畴而对他人有所'隐'，是任何发生个体意识、承认私人生活空间的社会都必须有的观念。"因为互联网服务商控制着用户的数据，所以隐私保护是其需要重点考虑的内容。

为了解决网络用户身份隐私的问题，真实用户身份需要转换为匿名或者伪身份(Anonymous/Pseudo ID)是关键，即用户身份数据匿名化。同时在真实身份的匿名化或者伪身份的生成过程中，可以采用定时更新机制。通过这种更新防御机制，可以有效挫败攻击者通过累积密文获取足够信息的攻击方法。确保大数据服务合作伙伴只能获得相应的用户的部分信息，而非用户的所有信息。用户隐私保护的大数据技术一般包括如下内容。

(1) 无人工的全机器自动处理。

(2) 统计数据而非个体数据。

(3) 安全加密的数据库，如 CryptDB。

(4) 采用同态加密技术(Homomorphic Encryption)。

2.2 计算机系统产业

计算机系统产业是一个生态系统(Ecosystem)，其中著名的大公司如下。

(1) 芯片设计商：Intel、AMD、TI、NVidia、VIA 等。

(2) 芯片制造商：台积电、Intel、MTK(联发科)、中芯国际等。

(3) 主板集成商：Intel、华硕、Acer、富士康等。

(4) 软件提供商：Microsoft、IBM、Oracle 等。

计算机系统产业是一个完整的工业链(Industrial Product Chain)，有上、中、下游产品之分，下游厂商集成上游厂商生产的组件构造新的组件，最后组成服务产品，向终

端零售商供货，最后交付给实际用户。

2.3 计算机网络产业

计算机网络产业是一个生态系统（Ecosystem），其特征是网络系统是一个基础设施，基于计算机系统，每个组件都是计算机系统。

由组件构造新的组件，最后组成服务产品，符合人类不断建造更大、更可用系统的内在动力，不断增强人类的计算能力与自动化能力。

1. 网络设备商

网络设备商一般都是大公司，主要包括如下上市或即将上市公司。

（1）芯片供应商：Intel、Broadcom、Marvel、PMC 等。

（2）设备提供商：思科、瞻博、华为、中兴等。

（3）无线系统解决商：艾诺威 AreoHive、思科等。

（4）无线路由器：普联（TP-Link）、小米、华为等。

2. 网络运营商

基础网络运营商一般都是垄断性企业，包括如下上市的国内外企业。

国内：中国移动、中国联通、中国电信、中国教育科研网和长城网（军方）等。

国外：Sprint、AT&T Verizon、T-mobile、Comcast、DoCoMo、NTT、BT 和 Orange 等。

3. 网络服务商

类似于传统工业的制造业、零售业和服务业，依托计算机网络构建的基础框架设施提供了面向最终用户的多方面的计算机网络服务产业。

面向最终用户的服务类大公司如下。

（1）数据中心：IDC、世纪互联等。

（2）搜索公司：谷歌、百度、搜狗等。

（3）门户网站：新浪、搜狐、雅虎等。

（4）即时通信：QQ、微信、SKYPE、AOL 等。

（5）电子商务：亚马逊、阿里巴巴、京东、当当等。

（6）社交网络：Facebook、领英 LinkedIn、人人、微博等。

（7）网络游戏：腾讯游戏、YY 欢聚时代、盛大、网易、九城等。

面向最终用户的服务的中小规模公司，通过定制系统、定制服务等方式紧密结合需求，是很多创业公司的发展模式。

2.4 IT 产 业

IT 产业一般分为计算机工业和通信工业，计算机工业一般指计算机系统产业计算机终端、计算机网络产业和计算机网络服务产业。

而通信工业，包括无线电信网络、传统固化网络和电信通信终端等产业。

（1）计算机硬件类：英特尔、ARM、AMD、苹果、联想等。

（2）计算机软件类：微软、甲骨文等。

（3）网络设备类：思科、Juniper、华为、中兴等。

（4）网络运营类：中国联通、中国移动、中国电信等。

（5）网络服务类：谷歌、百度、腾讯、阿里巴巴、雅虎等。

（6）通信工业：Alcatel-Lucent、Nokia-Siemens、Ericsson、HuaWei、ZTE 等。

第 3 章　互联网是什么

前面提到了互联网的安全性，为了说明其深层的原因，下面进一步对互联网工作的基本原理进行简要介绍。

3.1　互联网结构

解决人与人之间的通信问题，最基本的手段是给每对人之间都拉上专线光纤，形成点到点网络，如图 3.1 所示。这样，全世界有 N 个人，就需要 C_N^2 条专线。但是因为专线经济成本太高，这是不可行的，所以需要先设计部署一个本地接入网络，人人先接入局部网络（或叫局域网，对于世界范围，局部也是相对的），然后由路由器（Router）将这些小网络连接起来，形成更大范围的网络，这就是 Internet 的基本结构，如图 3.2 所示。图 3.3 为实际的互联网结构，其中分为国家骨干网、ISP 的区域接入网、每家每户的局域网等。

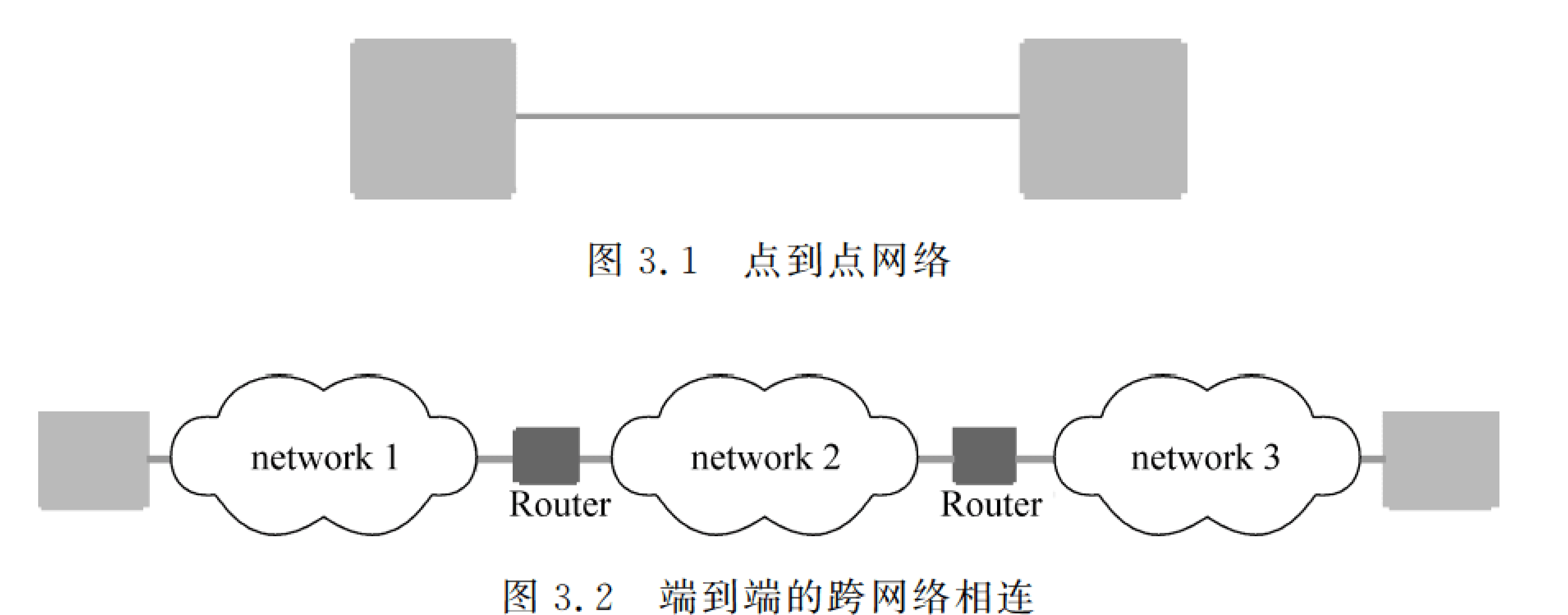


图 3.1　点到点网络

图 3.2　端到端的跨网络相连

ISP
互联网服务接入商
骨干网
Backbone
ISP
互联网服务接入商

图 3.3　实际的互联网拓扑图

互联网在传递信息时，单条消息被划分为多个数据块，并以其作为传输单位进行发送，每个小块可能会沿着不同的路径在一个或多个网络中传输，并在目的地实施重组，

这些小块就是“网包”。协议是规定路由器能识别网包的格式与操作的动作。互联网传输基于 TCP/IP,TCP/IP 协议簇中将网络的网包因其包含信息不同,分为 IP 网包、传输层 TCP/UDP 网包和应用层网包。

互联网采用的 TCP/IP 由 Vinton G. Cerf 和 Robert E. Kahn 于 20 世纪 70 年代设计,并于 1980 年 9 月公布为 IETF RFC 791 标准。TCP/IP 为不同的数据网络(局域网、城域网和广域网)提供了一套标准的数据交换协议,使得不同的数据网络按照这一套标准语义和语法,能够建立路由和通信。为此,TCP/IP 设计者 Vinton G. Cerf 和 Robert E. Kahn 获得了 2004 年度 ACM 的图灵奖,此前他们分别获得 1994 年和 1996 年的 ACM SIGCOMM 终生成就奖。

3.2 运作原理

互联网的设计与人类社会运行几千年的邮政系统是一致的。正如人们书写信函一样,我们只要将内容写好,装上信封,写上收信人地址和寄信人地址及其邮政编码,投入邮局的任何一个邮箱就可以了。互联网采用的工作模式和邮政系统的运作模式类似,如图 3.4 所示。

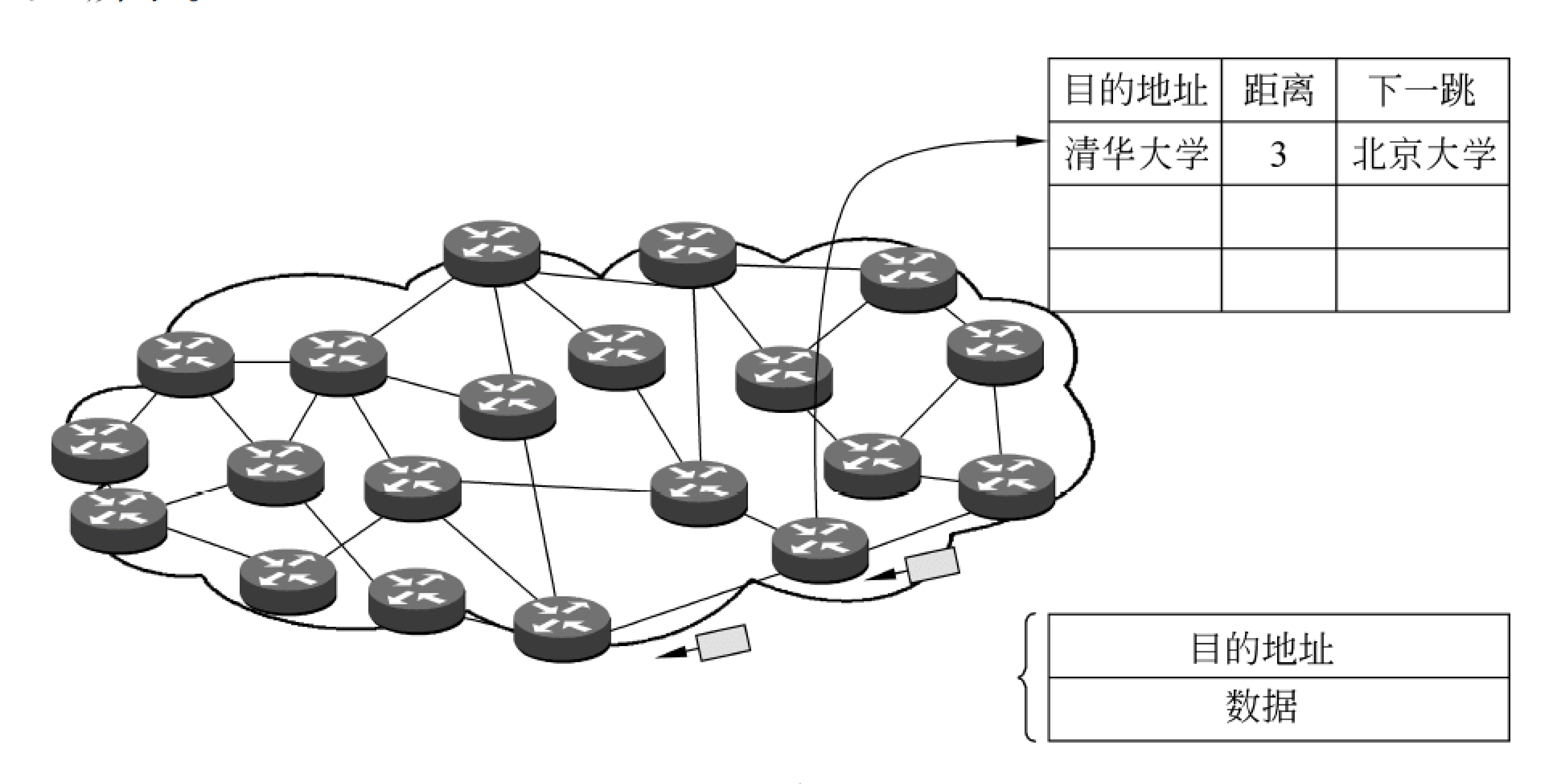


图 3.4 路由原理

首先,互联网地址分配机构 IANA 通过编址为全世界的计算机都分配一个 IP 地址(固定地址,类比于收信人和寄信人地址),IP 地址中包含该计算机所在区域号(即 IP 地址的网络地址,类比于邮政编码),以及在该区域内的详细地址,即主机地址(Host Address)。

其次,用户要发送的消息分解成许多网包(类比于一封封信函),送给的第一个路由器称为网关(也称为默认网关,类比于邮局邮箱)。路由器先在本地保存这份数据,然后等待机会发送到下一跳的路由器上,这样一跳一跳地向前路由(这种模式称为存储转发,类比于邮政职工将信件从一个邮局送往下一个邮局)。

如何确定信件的下一个路由器?这需要 IP 网络的路由系统(Routing System)来

确定。路由系统确定了从 A 点到 B 点路由过程中的传输路径,它是通过在每个路由器上维护一张路由表来实现的。每个路由器独立维护自己的路由表。每个路由器都会主动向邻居路由器通报自己的路由表信息,根据相邻的路由器的路由表来更新自己的路由表。

当一个网包到达之后,根据网包的目的地址信息,通过查找路由表信息,就可以将这份数据传送到下一个路由器上,一跳一跳地向前最终到达目的计算机上,在目的计算机上进行数据重组,呈现给用户。

这样就完成了信息从 A 点计算机转移到 B 点计算机的过程。以上网包交换过程,最初由 Paul Baran 于 20 世纪 60 年代提出,为此他于 1989 年获得了第一届 ACM SIGCOMM 奖。

3.3 域名系统

互联网通过所有计算机遵守 TCP/IP 完成了信息在 A 点计算机和 B 点计算机之间的数据传送。但是,标识机器的 IP 地址不易记忆,需要将机器地址转换为人容易识别的字串,域名系统就是互联网的人机接口,它负责机器地址与域名之间的映射。

20 世纪 90 年代专门用于提供信息内容的计算机出现了。这些信息的内容如何显示与创建、发布的规范,就是 W3C 的 WWW 标准。浏览器是显示这些标准格式内容的软件。随着浏览器的普及,以 W3C 为标准的 HTML 的 Web 内容越来越多,这时提供这些 Web 内容的网站也越来越多,如谷歌、新浪、搜狐等门户网站。怎么搜索定位这些内容的计算机就成了问题,比如如何将域名 www.sina.com 映射成 IP 地址,这就有了域名系统(Domain System),而存储这些域名与 IP 地址映射关系的机器就是域名服务器。

互联网的内容通过域名系统就能够精确定位,从而形成了一个提供内容和服务的互联网,这才是互联网最重要的用处,也就是“上网冲浪”的意义。

现在广泛使用的域名系统,最初由 Paul Mockapetris 设计完成,为此他于 2005 年获得了 ACM SIGCOMM 奖。

3.4 路由系统

路由系统就是互联网的交通运输通道,将一个机器上的信息传送到别的机器上。每个网包都具有独立的发信人地址和寄信人地址,因此路由器对这样的网包进行独立路由选择,互联网的信息传送和信息选路是同步进行的。

首先,IP 网络中的每个遵循 IP 的机器都是一个路由器,根据路由表来转发数据,如果路由表项的下一条是自己,则说明自己是这个信息的接收者,否则的话,就尽力把信息传送给其他路由器,如默认网关路由器或者其他相邻路由器。

其次,对于用户而言,互联网的路由系统是不可见的,用户只要配置好自己的默认

路由器就可以实现网络服务的接入，因此是没有网络接入访问控制的。

互联网的路由系统也是分布式的，按照网络管理域分为域间路由和域内路由。分别采用不同的路由协议来更新每个路由器的路由表。每个路由器运行路由协议，互相交换路由信息，如 OSPF 协议、RIP 和 BGSP 等。

3.5　TCP/IP

互联网的成功，很大程度上归功于采用了 IP 和坚持了"终端到终端"（E2E）互操作性及连接支持的设计原则的互联网架构。TCP/IP 为 IETF 标准。

3.5.1　互联网"细腰"

当今互联网的协议簇是一个沙漏模型（见图 3.5），其中处于"瘦腰"处的是 IP，它是互连互通的核心。而在 IP 之上的是 TCP 和 UDP，两者是互联网的主要传输协议，而又以 TCP 设计最为精巧。因此，整个互联网协议簇又称为 TCP/IP 协议簇。

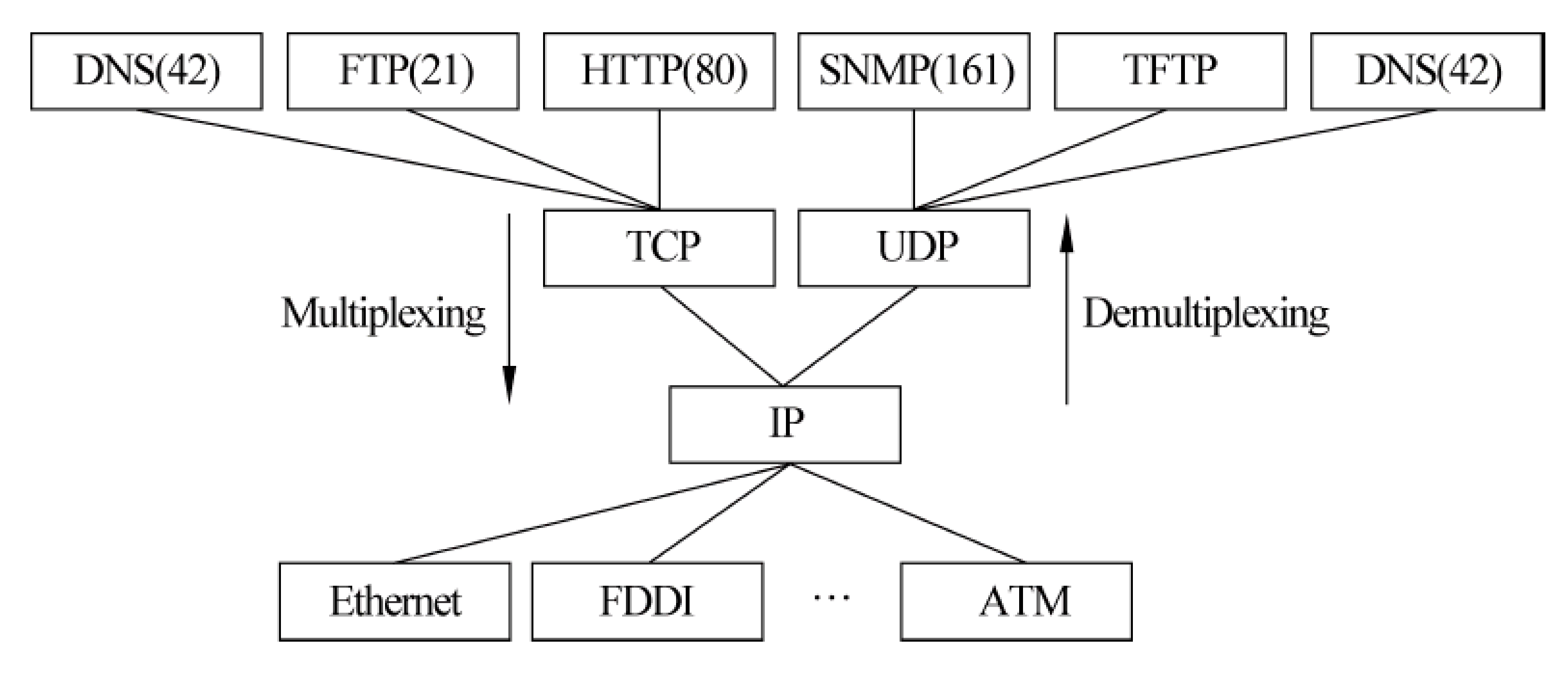


图 3.5　互联网协议图

3.5.2　IP

IP（Internet Protocol）是网络层协议，它尽力传送数据到达指定地址，不确认数据是否能正确到达，是一种无连接（Connectionless）的协议。IP 的最重要内容是为每台主机分配可路由的 IP 地址，主要由 DHCP（动态路由地址分配协议）完成。

1. 网包格式

IP 网包就是普通书面信函的信封，其格式如图 3.6 所示。信封内装的是信纸，就是这里的数据（data）。

IP 包的格式包括包头和包载荷两大部分。主要有如下字段组成：版本（4b）、首部长度（4b）、服务类型（8b）、总长度（16b）、标识（16b）、标志（3b）、片偏移（13b）、生存时间（8b）、协议（8b）、首部检验和（16b）、源地址（32b）、目的地址（32b）。

为什么寄信人的地址要写在收信人之前呢？因为 IP 是美国人设计的，大家可以注意一下西方的普通书信格式是寄信人在前，收信人在后，体现对收信人的礼貌，因此这

0	4	8	12	16	20	24	28	32
4b Version	4b Header Length	8b Type of Service		16b Total Length (B)				
16b Identification				3b Flags	13b Fragment Offset			
8b Time to Live (TTL)		8b Protocol		16b Header Checksum				
32b Source IP Address								
32b Destination IP Address								
Options								
Data								

图 3.6 IPv4 协议头

种设计就是文化传统的问题，如果让中国人来设计的话，可能就把这两个项给颠倒过来了。

2. IP 地址

当前 IP 版本 4(或简称 IPv4)用 IP 地址辨别互联网上设备或主机唯一的识别码，具有全局效应，适用于不同网络间寻址。

IP 地址由 32 位组成，理论上讲可有 2^{32}(4 294 967 296)个地址。

IP 地址采用分层结构，由网络地址(Network Address)和主机地址(Host Address)两部分组成。依照网络地址和主机地址的分配，分成 5 类地址。分成 5 类地址的主要原因是网络的规模(内部的计算机数目)多种多样，如图 3.7 所示。

		1st Byte	2nd Byte	3rd Byte	4th Byte	hosts
Class A	0	Network Address	Host Address			16 777 216
Class B	10	Network Address		Host Address		65 536
Class C	110	Network Address			Host Address	256
Class D	111	Multicast Multicast				Multicast
Class E	1111	Reserved				Reserved

图 3.7 IP 地址的分类

清华大学的 IP 地址为 59.66.0.1/16(A 类)、166.111.0.1/16(B 类)。采用 ipconfig 命令可以有效地确定 IP 地址。

```
C:\Users\zhenchen> ipconfig
Windows IP配置
```

以太网适配器 Local Area Connection:

```
连接特定的 DNS 后缀…… : tsinghua.edu.cn
IPv4 地址………………… : 166.111.137.197
```

子网掩码……………………：255.255.255.0
默认网关…………………… ：166.111.137.1

3. 子网掩码

如何获取 IP 地址的网络地址呢？这个问题由子网掩码(Subnet Mask)来解决，如图 3.8 所示。

IP Address	11000000	10101000	00000001	01110100
	←——— 27b ———→			
Subnet Mask AND	11111111	11111111	11111111	11100000
netid	11000000	10101000	00000001	01100000
	192 ·	168 ·	1 ·	96

图 3.8　子网掩码

4. 分割子网

将一较大的网络区段切割成几组较小的网络，称为子网化(Subnetting)，使用于内部路由选择协议(Interior Routing Protocol)进行路由交换。

例如，B 级网络 59.66.0.0/16 可拆分成如下 256 个较小的网络。

59.66.0.0/24
59.66.1.0/24
59.66.2.0/24
⋮
59.66.255.0/24

3.5.3 数据传输协议

1. 应用端口

IP 使得互联网上的任何两台计算机之间能够建立尽力而为的通信，但是当计算机上的多个通信程序同时使用网络时，还需要在 IP 之上设计数据传输协议，并引入端口的概念来区分不同通信应用程序。

IP 网络类比于邮政系统，如在信件传递的基础上，邮政系统又推出了快件、加急快件服务(如 EMS)、平信和挂号信等服务。类比于互联网，互联网的 TCP 和 UDP 就是在普通信件服务上增加的这些专用的服务，以保证不同业务的服务要求。

IP 之上的数据传输协议主要包括 TCP 和 UDP。应用程序在互相通信时需要选择数据传输协议 TCP 或者 UDP，以及相应的传输端口，以区别其他应用程序，如图 3.9 所示。

2. TCP

IP 使得 IP 网络上的任何两台计算机之间能够建立尽力而为的通信，为了在 IP 网

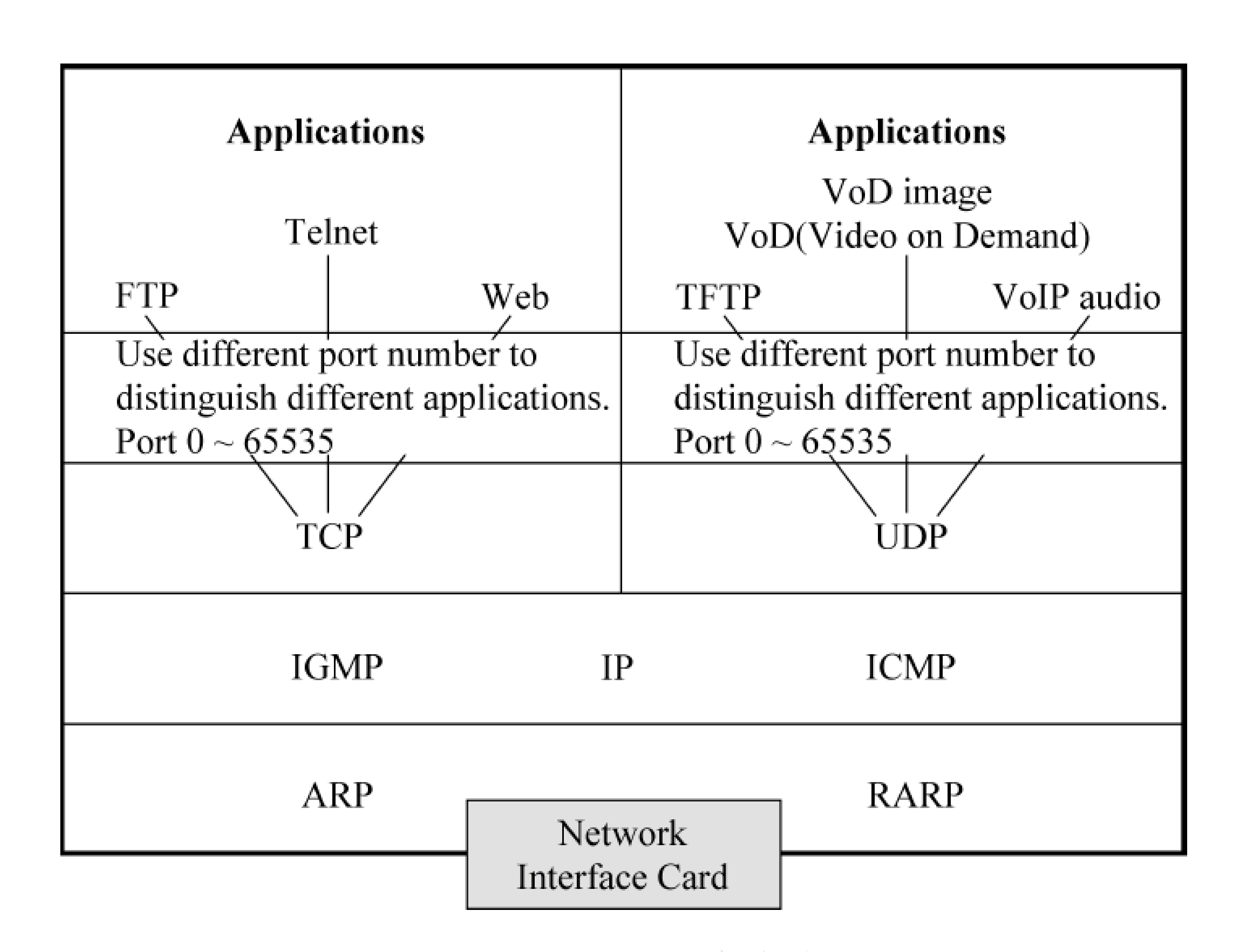


图 3.9 TCP/IP 协议栈

络偶尔存在丢包的情况下还能有效保障传输的质量(如文件传输服务),需要解决可靠传输问题。有时从 FTP 服务器下载电影需要将一个 1GB 大的电影文件分成很多网包在网络上传输,如果其中一份数据丢失将导致整个文件无法打开(因为校验不通过)。

为了解决可靠传输的问题,传输控制协议(Transmission Control Protocol,TCP)被提出,其基本思想是为每次通信会话保留状态,为传输的每段数据编号,通过发送和接收端的互相通报以及保存的状态信息来确定可能的网包丢失情况,通过重新传输丢弃的网包来保证可靠性。

图 3.12 是 TCP 包头的格式,包括包头和包载荷两大部分。主要由如下字段组成:源端口(16b)、目的端口(16b)、序号(32b)、确认号(32b)、数据偏移(4b)、保留(6b)、紧急位 URG、确认位 ACK、复位位 RST、同步位 SYN、终止位 FIN、窗口(16b)、校验和(16b)、紧急指针(16b)、选项字段、填充字段。

TCP 提供以下 3 个基本功能。

(1) 可靠性(Reliability):克服包丢失问题,传送的数据依照顺序交给程序。

(2) 复用性(Multiplexing):通过不同的端口可使同一个 IP 地址(一台计算机)可以同时提供上层不同的多种服务,如 FTP、Telnet、HTTP Web 服务等。

(3) 流控(Flow Control 或 Congestion Avoidance and Control):避免网络或接收端拥塞,以便提供有效率的传输。

TCP 的会话称为连接(Connection),TCP 的会话建立需要三次握手,会话拆除也需要握手,如图 3.10 所示。这种握手协议也是 TCP SYN 泛洪攻击的原因,如图 3.11 所示。

TCP 流量控制是其关键技术之一,该问题最初由 Van Jacobson 提出和解决,为此他于 2001 年获得 ACM SIGCOMM 奖。

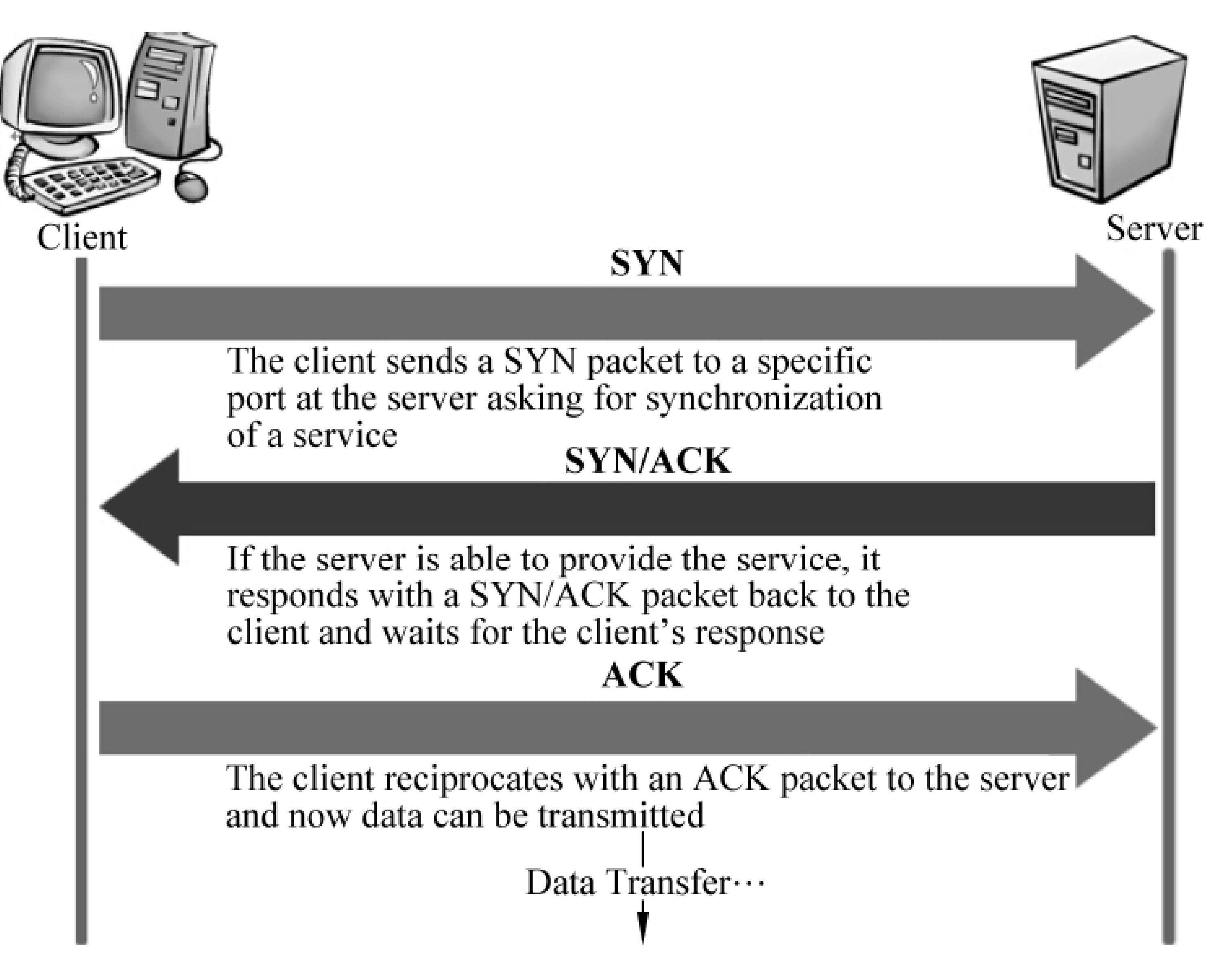


图 3.10　TCP 协议的三次握手

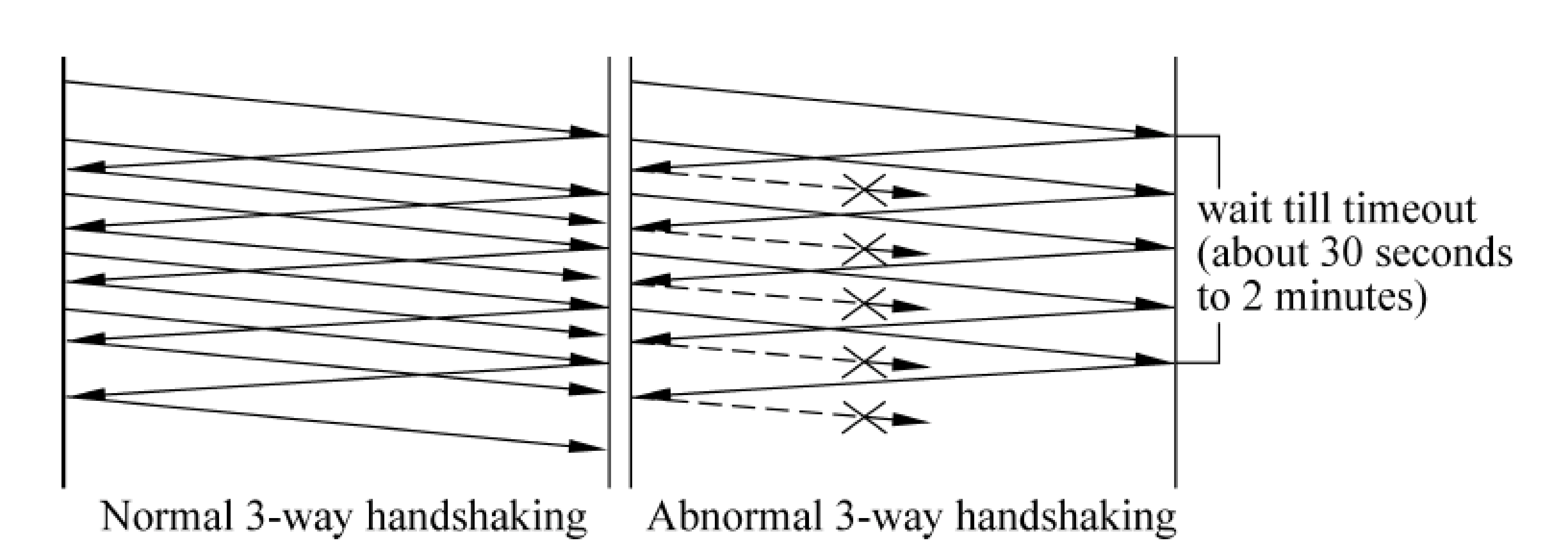


图 3.11　一种异常的 TCP SYN 泛洪攻击

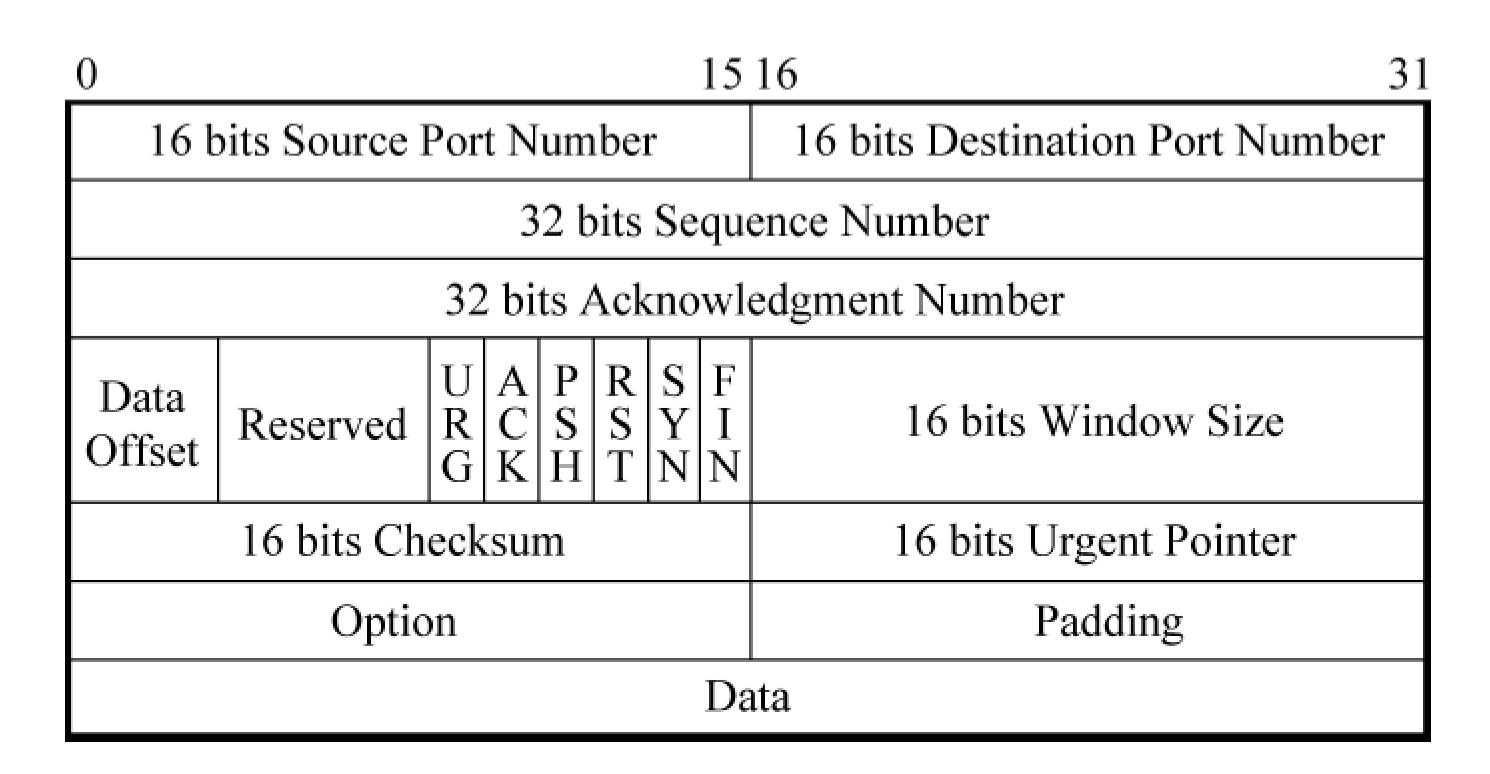


图 3.12　TCP 包头的格式

3. UDP

IP 使得 IP 网络上的任何两台计算机之间能够建立尽力而为的通信，讲究传输速度且允许一点数据丢失(Data Loss)或是数据包丢失(Packet Loss)的常用传输协议是用户数据包协议(User Datagram Protocol，UDP)。例如 QQ、GTalk、Skype 等使用语

音通信的应用程序均使用了 UDP。

UDP 定义于 RFC 768,提供应用程序能够在最低的协议机制下发送消息给其他应用程序,但不保证是否可靠传送或有没有依照传送顺序到达。

图 3.13 是 UDP 包头的格式,包括包头和包载荷两大部分。主要由如下字段组成:源端口(16b)、目的端口(16b)、UDP 包长度(16b)、校验和(16b)。

0 15	16 31
16 bits source port number	16 bits destination port number
16 bits UDP length	16 bits UDP checksum
Data	

图 3.13 UDP 包头的格式

3.5.4 ICMP

互联网的运作离不开故障的管理,互联网控制消息协议(Internet Control Message Protocol,ICMP)用来处理网络设备之间的错误,报告网络环境中错误状态的发生,但是无法确保能把消息确实送达或是转回发送地。

ICMP 的一个重要应用是 Ping,它可用来测试两台主机之间的连通性。下面是在微软公司 Windows 的 DOS 环境下的例子

```
C:\Users\zhenchen> ping www.tsinghua.edu.cn
正在 Ping www.d.tsinghua.edu.cn [2001:da8:200:200::4:100] 从 2001:da8:200:900e:2
00:5efe:166.111.137.197 具有 32 字节的数据:
来自 2001:da8:200:200::4:100 的回复:时间<1ms
来自 2001:da8:200:200::4:100 的回复:时间<1ms
来自 2001:da8:200:200::4:100 的回复:时间<1ms
来自 2001:da8:200:200::4:100 的回复:时间<1ms
2001:da8:200:200::4:100 的 Ping 统计信息:
数据包:已发送=4,已接收=4,丢失=0(0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短=0ms,最长=0ms,平均=0ms
```

ICMP 的另外应用是 traceroute(Linux 环境)和 tracert(Windows 环境),它们可以用来分析两台主机之间通信通过的路由器。下面是在微软公司 Windows 的 DOS 环境下的 tracert 例子。

```
C:\Users\zhenchen> tracert www.berkeley.edu
通过最多 30 个跃点跟踪到 www.w3.berkeley.edu [169.229.131.81]的路由:
1    <1毫秒   <1毫秒   <1毫秒   SECURITY [192.168.128.1]
2    1 ms     <1毫秒   <1毫秒   166.111.137.1
3    <1毫秒   <1毫秒   <1毫秒   tu128098.ip.tsinghua.edu.cn [166.111.128.98]
4    1ms      <1毫秒   <1毫秒   tu128101.ip.tsinghua.edu.cn [166.111.128.101]
5    1ms      1ms      <1毫秒   th004133.ip.tsinghua.edu.cn [59.66.4.133]
```

```
6    4ms    1ms    1ms    118.229.2.10
7    1ms    1ms    1ms    118.229.2.14
8    1ms    1ms    1ms    118.229.2.2
9    10ms   11ms   11ms   th002237.ip.tsinghua.edu.cn [59.66.2.237]
10   11ms   11ms   10ms   pku0.cernet.net [202.112.38.73]
11   11ms   11ms   11ms   202.112.53.169
12   3ms    3ms    3ms    202.112.61.158
13   12ms   11ms   11ms   202.112.53.18
14   100ms  100ms  100ms  tpr5-ae0-25.jp.apan.net [203.181.194.125]
15   215ms  214ms  215ms  losa-tokyo-tp2.transpac2.net [192.203.116.145]
16   206ms  205ms  206ms  cenichpr-1-lo-jmb-702.lsanca.pacificwave.net
                          [207.231.240.129]
17   214ms  213ms  214ms  svl-hpr--lax-hpr-10ge.cenic .net[137.164.25.13]
18   215ms  215ms  215ms  oak-hpr--svl-hpr-10ge.cenic.net [137.164.25.9]
19   217ms  215ms  216ms  hpr-ucb-ge--oak-hpr.cenic.net [137.164.27.130]
20   225ms  225ms  225ms  t2-3.inr-202-reccev.Berkeley.EDU [128.32.0.39]
21   222ms  217ms  216ms  t1-1.inr-211-srb.Berkeley.EDU [128.32.255.43]
22   216ms  217ms  216ms  webfarm.Berkeley.EDU [169.229.131.81]
跟踪完成。
```

由此可见,从教育网的一台机器到达美国伯克利大学的网站服务器之间通过了22个路由器,中间还包括日本的节点。

3.6 以 太 网

1. 以太网是什么

以太网(Ethernet)是使用最广泛的局域网类型。10～100Mbps 以太网采用共享网络介质,属于共享带宽;吉比特以太网(Gigabit Ethernet)采用交换网络方式,属于独享型带宽。

无线以太网主要是 IEEE 802.11 标准。

2. 以太网协议

以太网协议见 RFC 894,以太网协议帧格式如图 3.14 所示。

3. 网线

以太网网线为 10Base-T 和 100Base-T,使用 8 芯(4 对线)的无遮蔽双绞线(Unshielded Twisted Pair,UTP)网络线,接头为 RJ-45。接法有平行接法和串接接法,具体连接关系如图 3.15 所示。

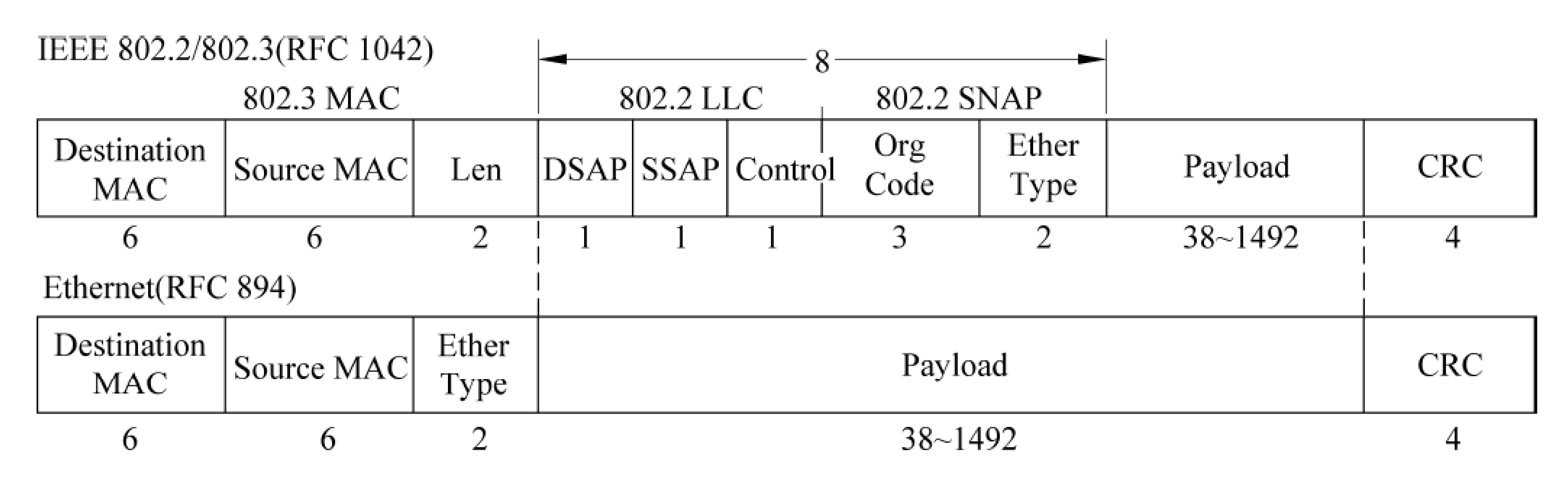


图 3.14　以太网协议帧格式

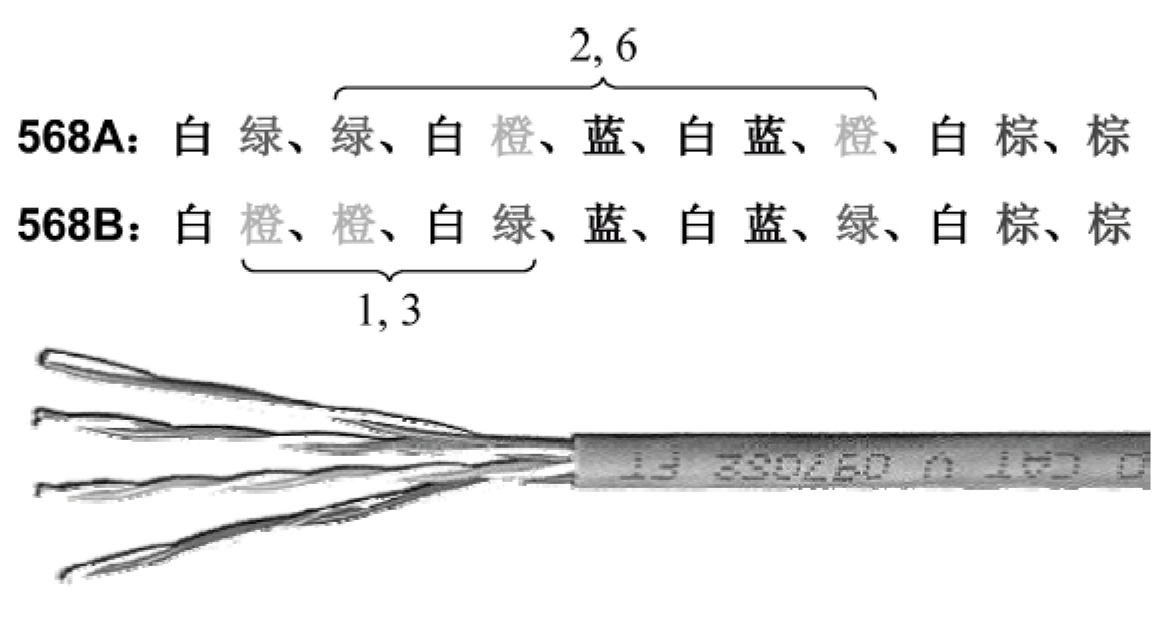


图 3.15　以太网 RJ-45 接口走线

3.7　重　叠　网

3.7.1　重叠网定义

重叠网或者覆盖网(Overlay Network)是一套部署在现有互联网上的服务器：①为一个或多个应用提供基础设施。②以与基本的互联网中相应部分不同的或者有竞争性的方式，来尽责地转发和处理应用数据。③可以由第三方在一个有组织和协调一致的方式下运作(其中可能包括最终用户的集合)。

覆盖网络技术为改善 IP 网上的服务质量提供了一种新的思路，这种解决方案易于推广，灵活性高。

因为覆盖网是利用现有基础设施构成的虚拟网络，因此也是网络虚拟化的一种形式。就如同现在电子商务的物流网络是建立在国家基础交通网络上的虚拟网，因此是一种覆盖网的形式。再如现在 Internet 上的 P2P 应用 BitTorrent、Donkey 和 Emule 等，Skype 公司的 VoIP 通信网络，网宿、蓝汛、Akamai 公司的 CDN(Content Delivery Network)等，均是覆盖网。

3.7.2　重叠网分类

覆盖网络有广义和狭义之分，在广义上，任何在一种底层网络组织结构上所抽象出来的逻辑网络结构，都可以称为覆盖网络。从这个意义上来说，由于 Internet 的 IP 层

可以将各种各样的、采用不同物理层实现和链路层协议的异质网络互连起来，并用一种统一的协议来定义整个网络的工作方式，因此可以把 IP 层视为各种底层网络的一个覆盖网络。

在狭义上，覆盖网络是指构建于 IP 层上的一种逻辑网络结构，可以是由应用程序本身实现的应用层网络，也可以是以中间件形式向上层应用提供服务的抽象网络。当前覆盖网络的研究方向主要分为面向特定应用的覆盖网络和通用的覆盖网络平台两种。

覆盖网络的出现使得 Internet 能够支持更多的业务和应用。目前在 CDN、P2P 文件共享和应用层组播、流媒体技术等应用中，都利用了覆盖网络技术。

3.7.3 内容分发网络

CDN 旨在帮助 Internet 上的内容提供商（网站）为用户提供更好的服务。CDN 将采用集中式存储方式的服务器用一个分布式的服务器集群来代替，这些服务器节点分布在各个主要的互联网接入点，组成了一个覆盖网络。该网络可以通过智能化的控制方式，将内容发布到距离用户最近的网络“边缘”节点上，使得用户能够快速地访问内容，获得较好的服务体验。不仅如此，CDN 还能够有效地减轻服务器的骨干网的工作负荷，使得网站可以支持更大规模的服务。

3.7.4 P2P 文件共享

在这种应用中数据被分布式地存储在对等节点（Peer）上，所有的对等节点就组成了一个覆盖网络。根据覆盖网络的拓扑结构，可以定义一种有效的搜索方式，使得用户能够快速地在网络中进行信息检索。与集中式存储模式相比，P2P 网络具有自组织性、可扩展性、健壮性以及负载均衡等优点。以下这些著名的 P2P 文件共享系统都采用了不同的覆盖网络拓扑结构：Napster 采用了基于中心索引的星型拓扑；Gnutella 是基于非结构化的网状拓扑；KaZaA 引入了“超级节点”，构成分层拓扑；而 OpenDHT 等基于 DHT（分布式哈希表）的系统则采用了多种精巧的覆盖网络拓扑，如链状结构的 Chord、树状结构的 Pastry 和二维平面结构的 CAN（Content Addressable Network）。

第 4 章　网 络 安 全

这里我们探讨一下互联网安全为什么会有这么多问题，其中互联网体系架构和软件系统脆弱性是网络安全一内一外的两大重要原因。

4.1　互 连 互 通

基于 TCP/IP 技术的互联网获得了巨大成功，战胜了通信工业提出的 ATM/X.25 等其他网络技术方案成为事实的计算机网络标准，成为人类社会的基础信息网络框架。同时，WWW 的兴起为互联网的内容提供了一种标准的媒体描述方式，使得互联网不仅仅是作为计算机网络而存在，同时是具有丰富的媒体内容资源，促进了互联网爆炸式的增长。在此基础上，随着信息化的浪潮，人类社会的社会行为纷纷迁移到了互联网上，形成了电子政务、电子商务、电子金融、电子教学等。当互联网的使用成为人类的生活习惯时，互联网安全问题才逐渐受到大家的关注，以致成为热点问题。

互联网技术作为传统电信网络的颠覆者，是一个开放的平台，从技术发展角度去考虑设计问题，提供了丰富的媒体内容，顺应用户的需求，顺应新事物由弱到强、由小到大的发展过程。互联网的成功主要有如下 3 点。

（1）从不可靠的网络出发，构建可靠的网络。

（2）从互信、未考虑安全因素出发，构建安全网络。

（3）从对等角度，构建大规模系统。

表 4.1 给出了电信网络与互联网的对比说明。

表 4.1　电信网络与互联网比较

	电 信 网 络	互　联　网
设计用途	话音传送为主	数据传输网络
服务内容	电话、传真、短信	网页、视频、多媒体等
设计目的	商业化、可运营化	健壮、抗毁、自愈
商业模式	收取通信费用	初期无商业化、多元化
设计要求	保证通信质量	尽力传送，保证互连互通
结构模式	同质，从上到下，集中管理	异质，对等，分布式，自治
发展模式	集中式架构，集中规范，集中升级	松散的联盟
网络终端	固定通话，终端地址	具有网络接口的计算机
设计理念	网络设计复杂，终端功能简单	网络简单，尽量把复杂功能留给终端

是否要重新设计 Internet？答案是肯定的，也就是设计下一代互联网或者未来网络。目前 IPv6 应用也越来越广阔，事实上，IPv6 只是新一代互联网的一种而已。

如何设计网络呢？这主要是架构与工程的问题，理论问题不多。事实上，从 2010 年开始，世界各国都兴起了新的网络设计热潮，美国国家自然科学基金（NSF）在 2010 年，一次资助了 4 个未来的互联网研究项目，以解决当前互联网存在的网络安全、移动性、应用僵化和可管理性等问题。我国在未来互联网研究中投资巨大，目前，清华大学已经和 NDN 项目组进行合作，以期在该领域有所斩获。其中最新潮的解决思路称为信息中心网络（Information Centric Networking，ICN），它强调信息内容的互连互通。这其中最引人注目的是命名数据网络 NDN/CCN（Named Data Networking/ Content Centric Networking），它由加州大学洛杉矶分校（UCLA）计算机科学系张丽霞教授领导 12 所学校联合开发。

4.2　系统脆弱性

随着计算机系统的功能越来越丰富，系统的规模越来越庞大，软硬件系统自身的健壮性由于系统的复杂性而降低，造成系统存在很多安全“漏洞”。在软件开发过程中，开发的复杂性通过编程语言、编程类库、编译工具和操作系统调用而大大增加了安全漏洞的产生。同时在商业化的竞争压力下，在系统的性能功能与安全性之间的平衡中，系统开发对安全功能的重视不够，因为安全的代价是以牺牲成本、性能和易用性为代价的。图 4.1（见 www.cert.org）展示了软件系统漏洞的增长趋势。

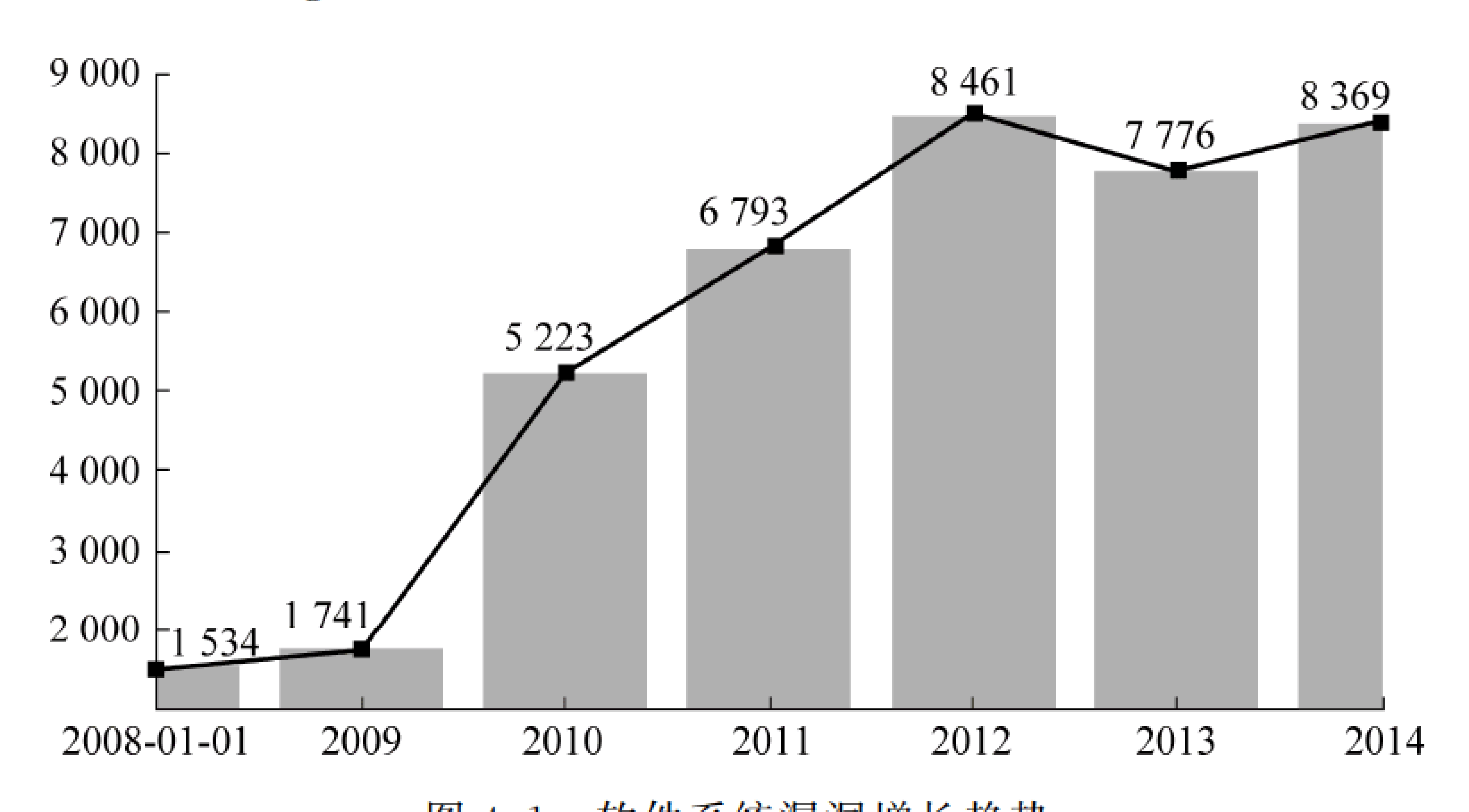


图 4.1　软件系统漏洞增长趋势

安全与用户友好性是一个比较大的矛盾：一个典型的案例是微软公司的 Windows XP，因其简单易用成为大众网吧的首选操作系统，因为其安全性比较低，但易用性极好；相反，Windows Vista 系统，吸收了 Windows XP 的安全问题，却因为过于重视安全性而导致易用性和性能下降，大大减少了用户的接受程度。因此，微软公司不得在 2009 年推出了 Windows 7，通过降低 Vista 系统的安全级别，已获得用户的易用性的认可。从这个例子可以看出，互联网安全有其根本性的原因（人的因素）。

零日攻击(zero-day)是指在软件补丁发布之日,恶意代码制作者通过反向分析补丁修补的漏洞,制作了针对该补丁修补的安全漏洞的攻击行为。这使得系统主机脆弱性的防御难度大大增加。

4.3 来自网络的攻击

随着计算机网络技术的不断普及,尤其是 Internet 成为信息基础框架,全世界的计算机采用 TCP/IP,通过路由器、交换机而连接起来,形成了全球互连互通的网络。这样,原本是单个计算机系统的安全漏洞通过网络的互连效应大大扩大了被攻击的可能性。

由于互联网是一个分布式的网络联盟,其体系架构中缺乏统一的安全和管理框架。开放的网络环境造成了攻击成本低,造成危害大的不利局面。松散的管理,比如 IP 地址的动态分配、IP 路径的重配置、网络地址的转换(NAT)、P2P 覆盖网络等技术,使得互联网安全事件的审计和追踪非常困难,追踪网络攻击受到管理域的范围限制,攻击行为不能得到应有的“惩戒”。

4.4 恶意代码的“黑金”

目前很多恶意代码,如木马(Torjan)、蠕虫(Worm)和机器人网络(Botnet)的背后都有地下经济的黑影。互联网安全事件从单纯的“找乐”、显示“个人成就”等动机,转化为经济利益驱动的具有黑金性质的地下产业。制作恶意代码,传播恶意代码,控制机器人网络,散发兜售广告邮件(SPAM)或者实施安全攻击,已成为一条完整的地下经济产业链。

加州大学伯克利分校的 Vern Paxson 教授研究表明,通过控制机器人网络来散发兜售药品的广告邮件,是成本收益比非常低的销售手段,从而为机器人网络扩散提供了很强的经济动机。

此外,通过控制机器人网络,对政府、商业等网站进行 DDoS 攻击,表达政治诉求或者谋求经济利益,也是互联网安全事件频发的因素之一。

4.5 网络安全是什么

网络安全是互联网中十分重要的方面,与现实生活中的安全问题一样,同样不可小视。在这个各种生产和消费活动都离不开网络的时代,小到个人,大到国家,都需要注意网络安全。网络安全,即采用网络设备或者软件,提供对计算机系统和计算机网络的保护,抵抗可能的破坏和风险。互联网安全是计算机控制权的攻防,是计算机网络世界中的较量,带有浓厚的“军备竞赛”(Arm Race)特征。

网络安全的特点是具有攻防两面性:攻击的方法都是细致入微,针对非常细致的

漏洞，属于案例研究；攻击防护比攻击要困难，属于“易攻难守”境况，这和网络环境相关。

网络知识是保障互联网安全的基础，知道攻击的知识，知道防守的办法才能具备良好的安全意识和物质技术保障。要做到这一点，首先要通过各种方式，使互联网使用者重视网络安全，了解互联网安全原理与技术的基础知识，在人们心中形成网络安全的初级防线。其次，互联网完全的维护要靠集体的力量。试想，纵使有很多人维护网络安全，只要有一小部分人还在无意识地成为传播木马、病毒等的工具，网络安全怎么能够保证？最后也是最为重要的一点，只有技术跟得上，人们才能与网络安全的破坏者真正抗衡。

4.6 互联网安全学科

互联网安全是信息通信安全的一部分，网络安全是信息安全、计算机系统和计算机网络学科相关联的综合学科，因此其涉及面广，工程性强，如图 4.2 所示。

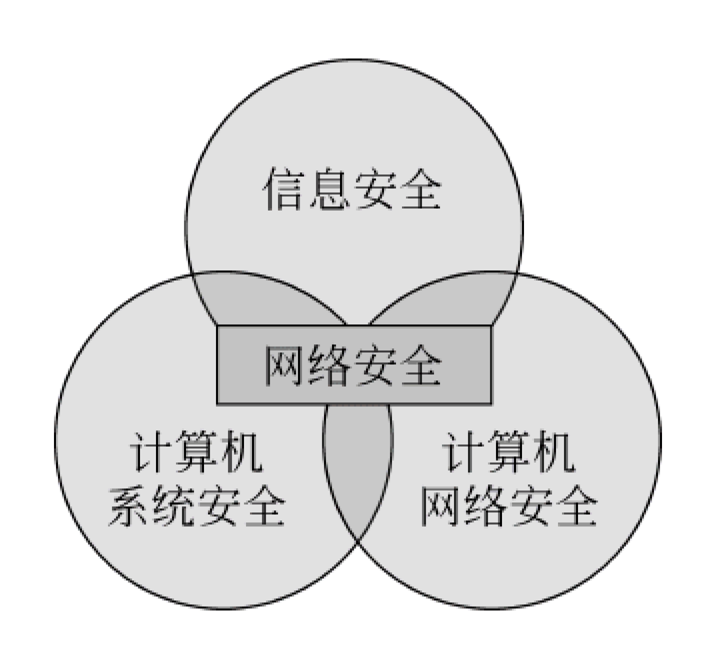


图 4.2 网络安全涉及计算机系统、计算机网络和信息安全

4.7 网络接入控制

网络接入控制(Network Access Control，NAC)是对计算机接入网络的控制协议。802.1x 就是 IEEE 为了解决基于端口的接入控制而定义的一个标准。802.1x 首先是一个认证协议，是一种对用户进行认证的方法和策略。它是对端口进行控制的。这里的端口可以是实际的物理端口，也可以是虚拟的 VLAN 端口。“基于端口的网络接入控制”是指在局域网接入设备的端口这一级对所接入的设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问局域网中的资源；如果不能通过认证，则无法访问局域网中的资源。

802.1x 体系结构如图 4.3 所示，包括 3 个实体：客户端、设备端和认证服务器。客户端一般是指网络终端，是需要接入网络的设备，客户端需要支持局域网上的可扩展认证协议(Extensible Authentication Protocol over LAN，EAPOL)，需要运行 802.1x 客户端软件，图中端口访问实体(Port Access Entity，PAE)是认证机制中负责执行算法

和协议操作的实体。设备端通常为支持 802.1x 协议的网络设备(如 H3C 系列交换机、思科系列无线接入点),它为客户端提供接入局域网的端口。认证服务器是为设备端提供认证服务的实体,用于实现用户的认证、授权和计费,通常为 RADIUS 服务器。

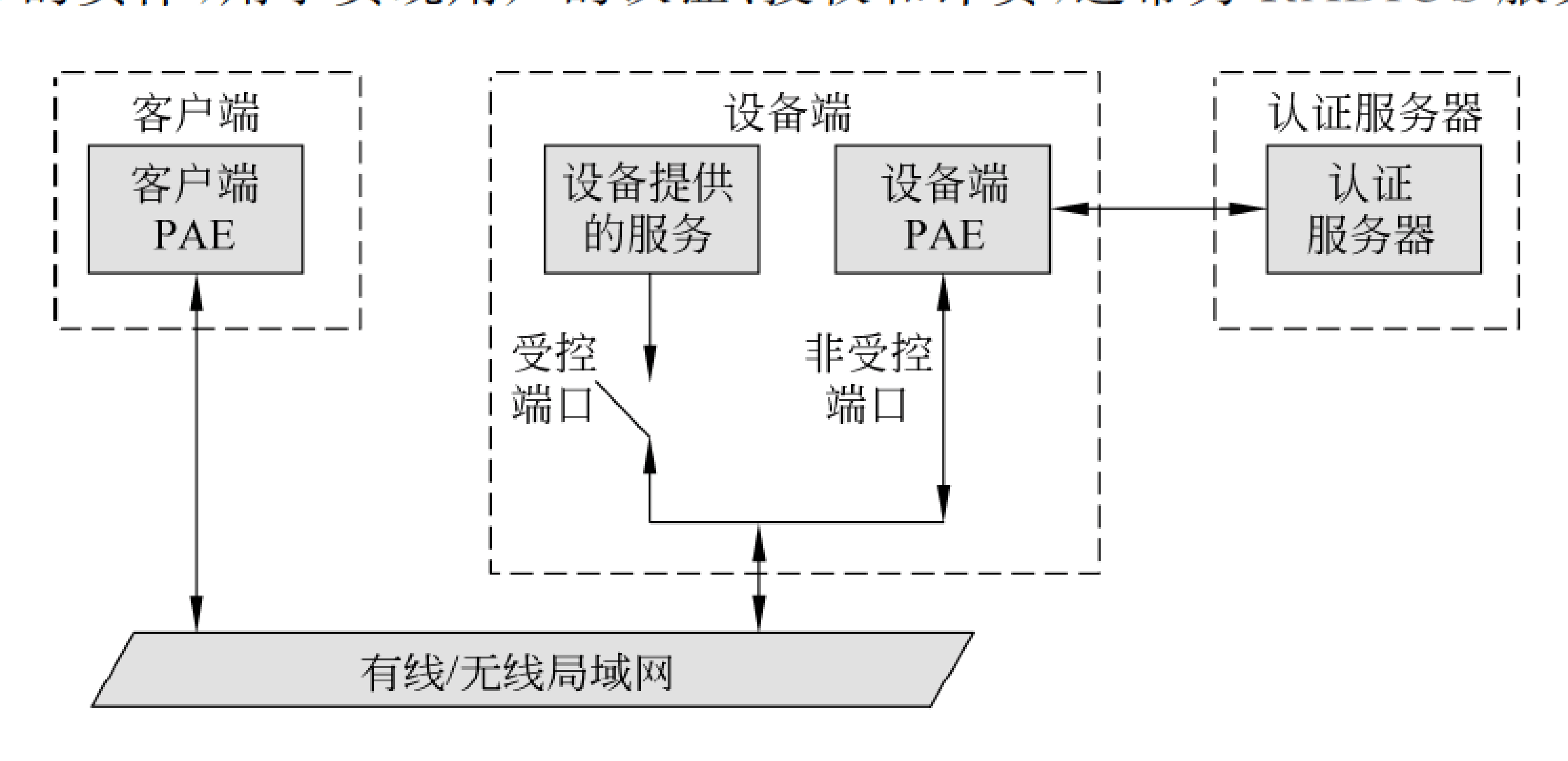


图 4.3　基于 802.1x 的网络接入原理

4.8　信息安全产业

信息安全产业包括计算机安全产业,计算机安全产业包括主机安全和网络安全,目前呈现两者的融合趋势,如图 4.4 所示。其中包括安全硬件、安全软件及各种安全服务,涵盖访问控制、身份认证、信息加密、安全威胁检测与保护等。



图 4.4　信息安全产品及服务

网络安全产业是 IT 产业不可缺少的部分,自从互联网高速发展以来逐渐被人们关注(1993 年至今)。网络安全利用软硬件系统阻挡来自网络的攻击,切实保障用户安全。互联网安全研究是计算机网络学科的分支,具有很强的实践性和工程性。

计算机安全工业是一个小生态，多姿多彩。由于这个产业的特殊性，所以对外大家可能不太了解。因为安全产业是一个“隐蔽”的产业，这也是造成这个行业的生态链具有比较封闭的特殊性。安全产业的监管部门有公安部、安全部、中央机要局和国家密码管理局、总参通信部。此外，各个行业有各自的安全产业、安全标准和服务，如金融业、电信业、交通业和政府部门等。

第 5 章　网络安全攻击

网络安全威胁主要有黑客攻击(Hacking)、恶意代码(Malware)、特洛伊木马(Trojans)、蠕虫病毒(Worms)、间谍软件(Spyware)和高级持续网络攻击(APT Attack)等。

5.1 黑客攻击

黑客攻击是以未经许可获取计算机控制权为目的的网络攻击。整个过程犹如特种部队作战,分为目标信息采集、锁定目标、目标攻击、隐匿善后等。在目标的采集上,对网络和主机进行探测,获取信息,或者由外入内,通过社交工程等方法。一旦锁定目标之后,即用各种安全工具(如 MetaPloit 等),或者特洛伊木马、病毒和蠕虫等,利用各种漏洞,如邮件服务、文件服务和网页服务等安全漏洞,获取目标的一定权限后,然后再用本地用户攻击等手段提升权限。入侵成功之后,隐藏后门,销毁痕迹,或者植入内核级的 Rootkit,以便以后进一步利用。

由于黑客攻击都比较隐秘,需要专门的安全流量审计来进行辅助分析,作者研究的协同式网络安全防御系统,旨在通过分布式部署流量探针设备,来发现可能的黑客攻击。

5.2 网络欺诈

网络欺诈也称为钓鱼攻击(Phishing Attack),是一种盗取用户银行或者电子商务账户的攻击方法,主要通过构建假冒的网页或者网站,利用垃圾邮件的散播,来吸引用户上当,比如声称用户的账户密码不安全,需要重新修改,或者发布中奖信息,吸引用户单击网络链接或者假冒邮件服务器管理员,让用户提交密码等。网络欺诈过程如图 5.1 所示。

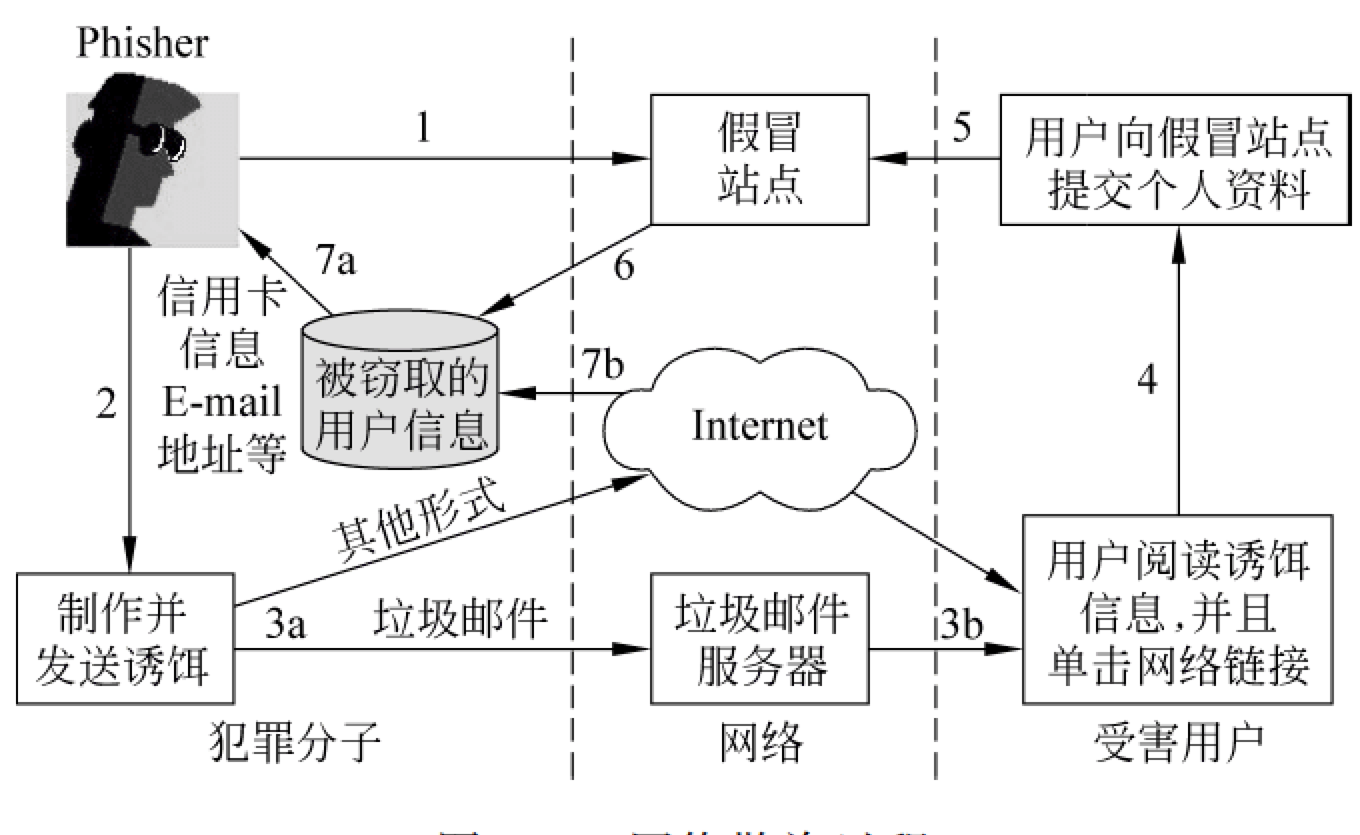


图 5.1　网络欺诈过程

网络欺诈目前已经形成了一条地下经济链条。各种攻击方法和手段日益成熟。在这条经济链条上,有着不同的分工,如构建假冒的网页或者网站,制作机器人软件,控制机器人网络,控制垃圾邮件的散播,每一个环节都从最终用户的损失中获得利益报酬,如图 5.2 所示。

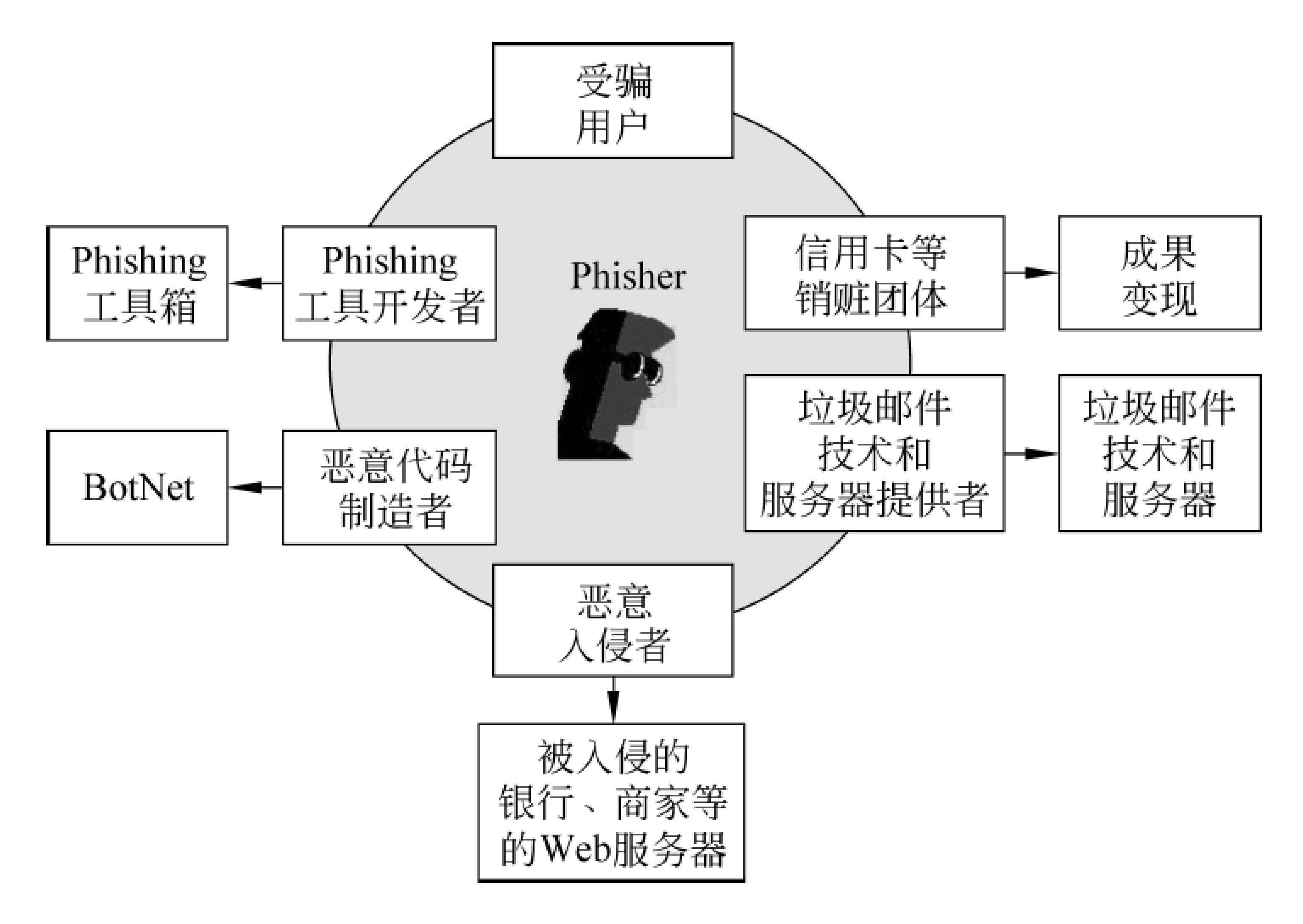


图 5.2　网络欺诈的价值链条

5.3　计算机恶意代码

中华人民共和国公安部第 51 号令《计算机病毒防治管理办法》于 2000 年 4 月 26 日颁布,其中计算机病毒(Virus)定义为:计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码。

更广义一些,计算机恶意代码(Malware)是指一个插入到系统中的程序(通常会故意隐匿),意图破坏受害人的数据、应用程序或操作系统的完整性、保密性和可用性,或者干扰或中断用户的正常使用。

恶意代码主要包括 4 种。

(1) 特洛伊木马是一种不能自我复制的程序,看似无害,实际上具有隐藏的恶意目的。

(2) 蠕虫是完全自包含、自复制的一段程序,不需要宿主程序就可以感染目标对象。

(3) 移动代码是从远程系统传输到本地执行的软件,一般不需要用户的明确指令,如 JavaScript 脚本代码。移动代码不感染文件,也不会自我复制,所以从根本上有别于病毒和蠕虫。不同于蠕虫会利用特定的系统漏洞,移动代码常常利用赋予其自身的系统默认特权来感染系统。

(4) 间谍软件是一种未经许可或用户知晓,在系统后台窃听用户网络使用状况,并

且收集或回传用户信息和用户行为信息的应用程序。

5.3.1 特洛伊木马

神话中，表面上特洛伊木马是“礼物”，实际上却是藏匿袭击特洛伊城的希腊士兵。现在，特洛伊木马是一些表面上有用的软件程序，实际目的是危害并破坏计算机安全。

木马实质是一个 Client/Server 程序，以远程访问控制受害机器，获取控制权和密码，并进行其他操作。其特点是作为不合法的网络服务程序，木马必须隐藏自己。

木马程序的传播方式一般为非主动传播，属于种植型。最近的特洛伊木马都以电子邮件的形式传播。

5.3.2 蠕虫病毒

蠕虫病毒可自动完成复制过程，控制计算机中传输文件或信息的功能，一旦计算机感染蠕虫病毒，蠕虫即可独自传播，并大量复制。

蠕虫病毒传播的特点是依靠网络主动传输，攻击受害机器，传播迅速，消耗极大的网络和计算资源。图 5.3 展示了蠕虫病毒的结构。

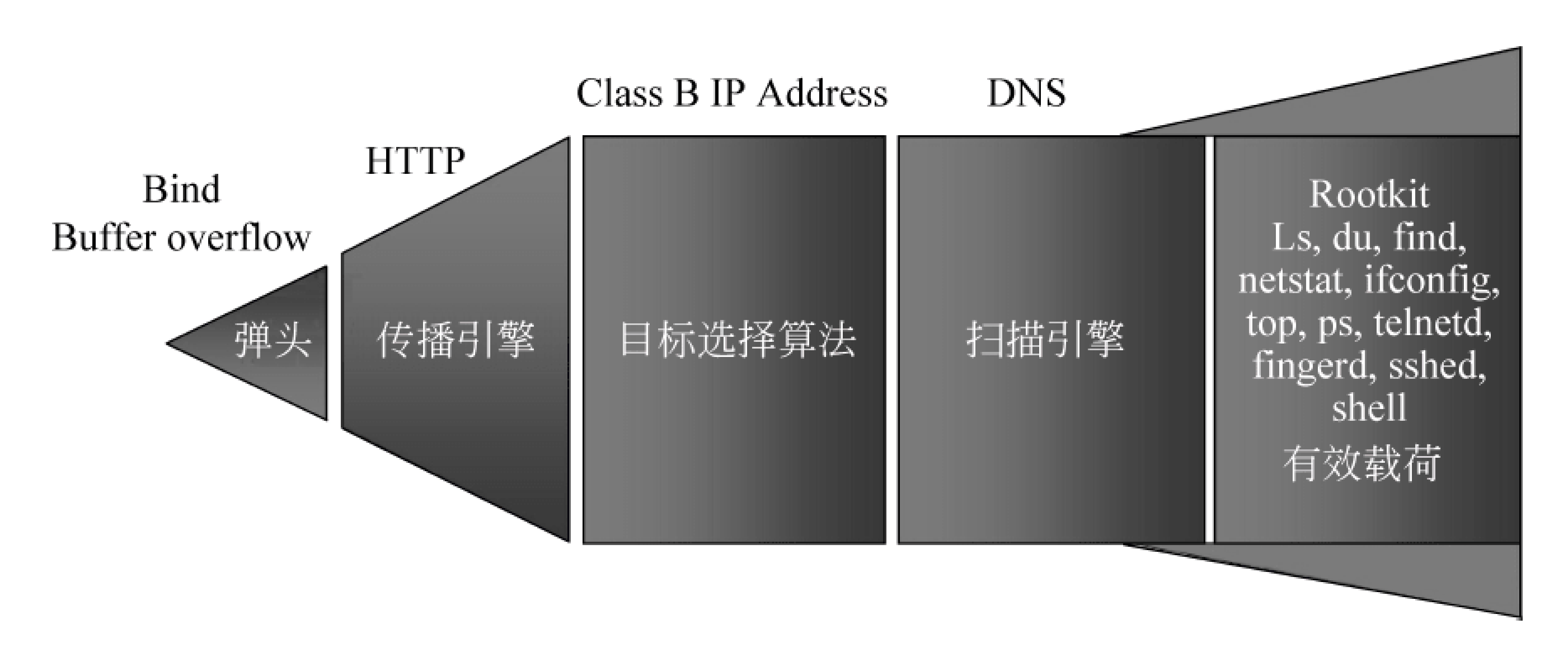


图 5.3　蠕虫病毒的结构

一个典型的例子是攻击 DNS Bind 服务器的蠕虫 Lion，它利用 Bind 程序的缓存溢出作为突破口，攻击 Bind 服务器，控制 Bind 服务器利用 HTTP 下载病毒体，确定 B 类 IP 地址作为攻击对象，进行传播。

最普遍的是红码病毒 CodeRed，且它具有多个不同版本，主要攻击 Windows XP IIS 系统漏洞，曾经风靡校园网络。

绝大多数蠕虫病毒主要是利用软件漏洞发布到漏洞补丁更新发布的时间差，从目前看，从软件漏洞发布到利用该漏洞的蠕虫出现的时间越来越多，近乎零日攻击(0day)，如图 5.4 所示。

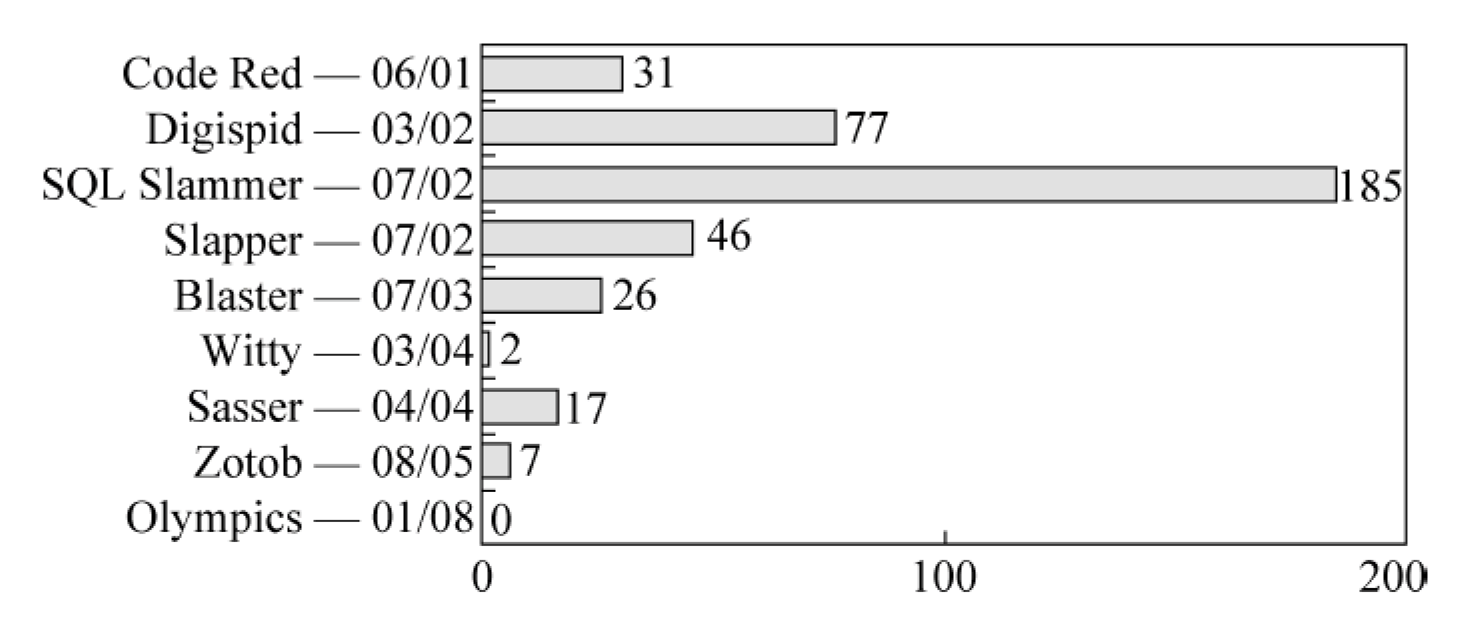


图 5.4　0day 零日现象——软件漏洞公布日及其利用的病毒的时延

5.4　机器人网络

机器人网络(Botnet)又称为僵尸网络、肉鸡网络。Bot 程序是一种恶意代码,能够创建后门程序,创建代理程序,转发邮件,记录键盘输入,获取口令、信用卡号码及其他信息,个别还能停止个人防火墙、杀毒软件等安全软件。Bot 程序一般会加壳保护,自动升级到新版本。

感染上 Bot 程序的机器,在用户不知情的情况下已经被黑客控制,所以俗称"肉鸡"。黑客一般通过 IRC 服务器发布控制命令操纵 Bot 机器,并利用 Bot 机器完成很多操作,比如攻击传播 Bot 程序。利用 Bot 进行时段出租,散发垃圾邮件,或者进行 DDoS 攻击等。目前发现的机器人网络规模最大可达数十万台机器,如图 5.5 所示。

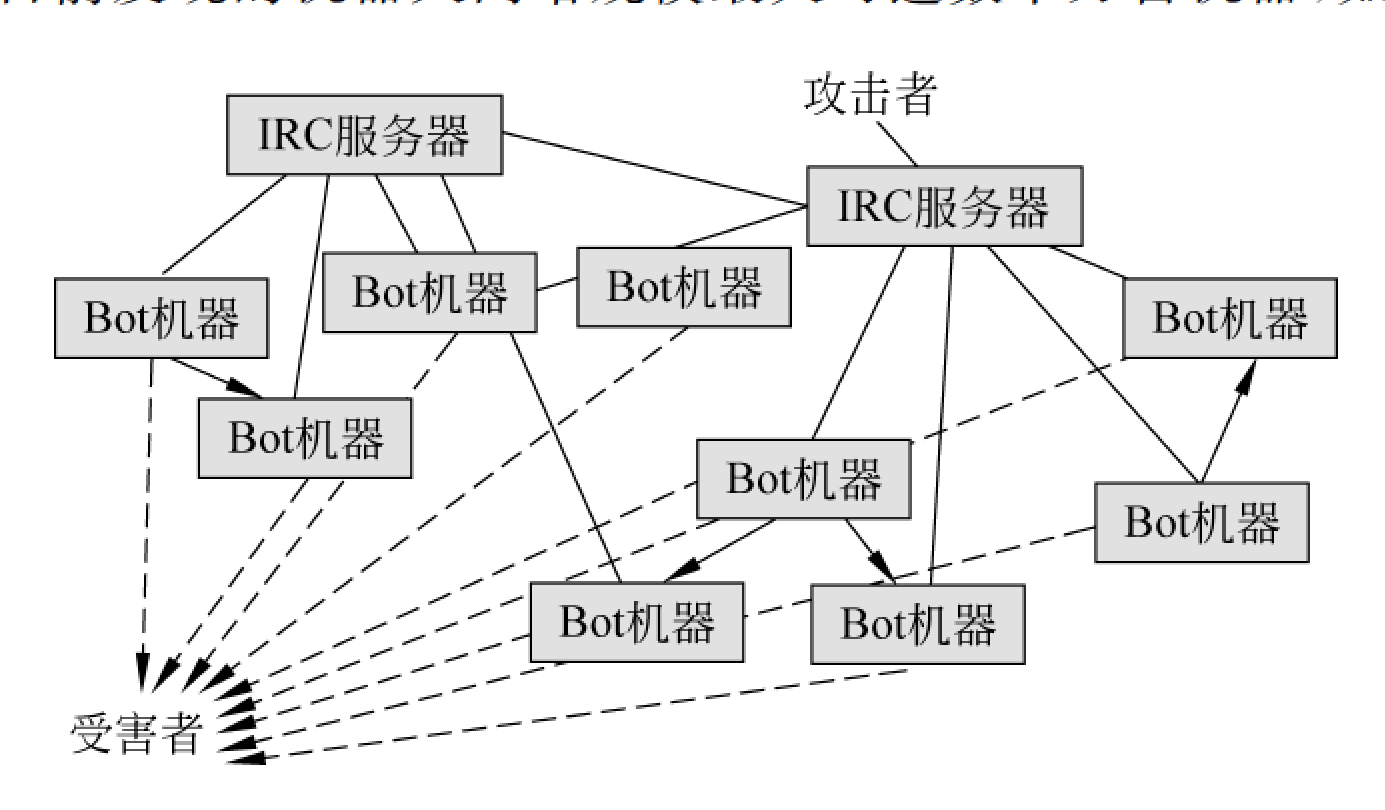


图 5.5　机器人网络发动 DDoS 攻击示意图

5.5　分布式拒绝服务攻击

拒绝服务攻击简称 DoS(Denial of Service),造成 DoS 的攻击行为被称为 DoS 攻击,其目的是使计算机或网络无法提供正常的服务。分布式拒绝服务攻击是网络中"没有硝烟的战争",攻击者利用客户端的计算机去充当僵尸网络中的僵尸机器,不断向受害服务器发送请求,占用了服务器处理请求的大量网络资源和计算能力,导致资源被消耗殆尽,无法处理正常请求。

常见的 DoS 攻击有两种。

(1) 网络带宽攻击。网络带宽攻击指以极大的通信量冲击网络,使得可用网络资源都被消耗殆尽,最后导致合法用户无法访问网络资源。

(2) 连通性攻击。连通性攻击指用大量连接请求冲击服务器,使得所有可用的操作系统资源都被消耗殆尽,最终使服务器无法再处理合法用户请求。

分布式拒绝服务攻击(Distributed Denial of Service,DDoS)指借助于客户/服务器技术,将多个计算机联合起来作为攻击平台,对一个或多个目标发动 DoS 攻击,从而成倍地放大提高拒绝服务攻击的威力。

攻击者使用一个偷窃账号将 DDoS 主控程序安装在一个计算机上,攻击者秘密安装代理程序到 Internet 的大量计算机上,代理程序能都对目标机器发动 DoS 攻击。利用客户/服务器技术,主控程序几乎同时激活运行成百上千的主机上的代理程序,控制代理程序对一个或多个目标发动 DoS 攻击。

根据我国刑法第 285 条和第 286 条、刑法修正案 7 和司法解释,恶意代码的制作、传播和使用是受限制的。

第 6 章　网络安全防范

互联网上的战争仍然在继续。互联网攻击行为不可能消失，而人们应对这种攻击的努力也不会停止，如何营造更加安全友好的互联网环境还需人们去解决。下面介绍网络安全防御的基本技术。

6.1　恶意代码防范

防范恶意代码要参考防范传染病的模式，如图 6.1 所示。类比了医学上防治传染病的原理，网络安全也要“预防为主，防治结合”；“综合措施，群防群治”；“加强监测，制止疫情”。其中切断传播途径是扼制恶意代码传播的主要方法。需要各种网络安全设备进行检测，分析以及协同配合。其中“易感人群”的预防，需要通过打补丁和加固来防治有安全漏洞机器的脆弱性。

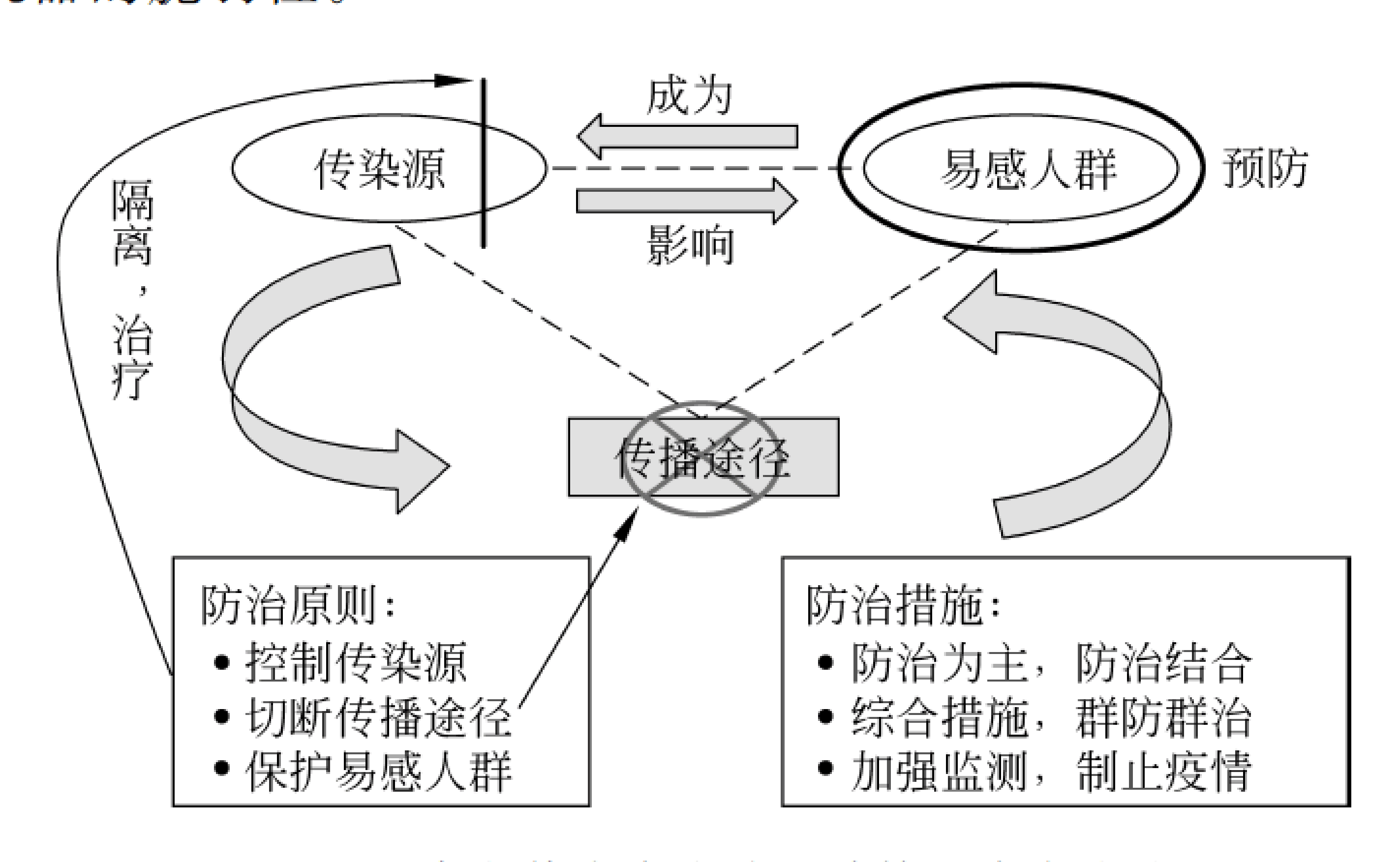


图 6.1　参考传染病防治的计算机病毒防范

从整体防御的角度看，安全防御包括终端侧的安全，防护网络侧的安全防护，以及一体化安全。

安装在主机上的客户端软件，检测发现恶意代码，同时不断地更新病毒库和安装补丁，用于预防可能的安全漏洞，并防御已经出现的新的恶意代码。

在网络流量入口或者关键点，部署防火墙或入侵检测系统。网络安全设备有大致分工，防火墙用于隔离，入侵检测系统用于分析，流量记录用于取证分析。

终端侧与网络侧的防御，通过网络访问控制结合起来，形成协同的一体化网络安全防御。

6.2　终端侧安全防范

6.2.1　杀毒软件

1. 病毒检测

在病毒发展猖獗的背景下，反病毒技术也在迅速发展。从当前的杀毒技术上来讲，反病毒软件的核心部分都是一个扫描器（scanner）。基于特征码的扫描方法是当前最主要的查杀病毒方式，它利用“特征码”检查文件、扇区和系统内存来查杀已知病毒。

同时，新的反病毒技术也正在研究、发展之中。由于互联网的普及，互联网已经成为病毒制作技术扩散、病毒传播的重要途径，病毒开发者之间已经出现了团队合作的趋势，病毒制作技术也在与黑客技术进行融合。这对现在的反病毒技术提出了挑战，反病毒技术正在发生转变，也就是说反病毒的技术正在从软件对抗向思想对抗进行转变。

之前的反病毒技术，只能在病毒出现之后再进行防范，对未知病毒几乎没有防范能力。而新的反病毒技术是基于对大量的病毒的特征、发作过程、传播变化统计的基础上，建立控制策略数学模型，采取分门别类的方法，有效解决应用同种思想开发出的各种病毒，可以极大地缩短对新病毒的反应时间。

由于这种方法是通过理解病毒设计思想而实现的，因此，这是一种病毒制造者与安全专家之间在整体思想层面的博弈竞赛。具体地讲，这些新型技术包括启发式扫描、行为判断等。行为判断就是通过驻留的杀毒软件截获那些对用户有病毒危险的行为，优点在于可以在病毒感染的早期发现并阻止。

利用虚拟硬件对未知病毒进行识别与清除的技术，其核心是以软件的形式虚拟CPU，如QEMU技术，然后将可疑文件放入这个虚拟的CPU进行解释执行，在执行的过程中对该可疑文件进行病毒的分析、判定。针对网络病毒，利用虚拟网络与虚拟主机技术，观察病毒在虚拟化环境中的执行，对其行为进行辨识和分析，如GQ系统等。

2. 病毒特征获取

杀毒软件最核心的内容是获取恶意代码的特征（Signature），恶意代码样本的收集是用户端杀毒软件的特征库更新的基础，如图6.2所示。通过密罐捕捉、垃圾邮件收集、爬虫等技术从互联网、企业收集恶意代码样本。

杀毒软件公司一般通过全球部署蜜罐网络来捕捉恶意代码，收集杀软从用户端上传的恶意代码等文件，进行分析，从而提取标识特征。杀毒软件主要有360、百度杀毒、Symantec、Mcafee、NOD32、Kaperskey等。

当前，杀毒软件公司越来越多采用云查杀的功能，通过沙箱sandbox技术，模拟执行代码，分析其行为，以判断性质，然后将可疑代码从用户计算机中上传到云中心，进行深入分析。

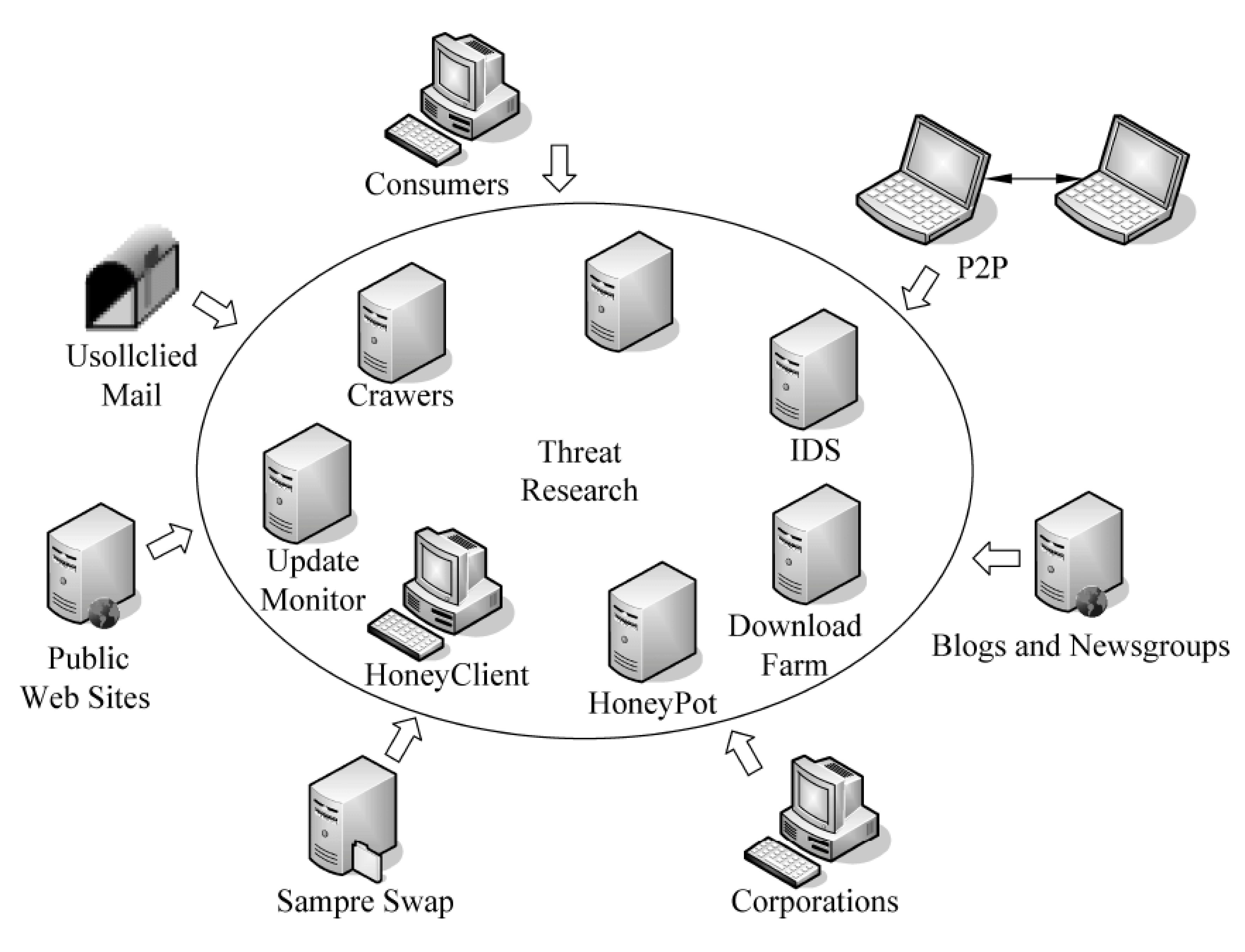


图 6.2　杀毒软件公司病毒特征库采集流程

在分析生成特征之后，生成病毒特征更新包，下载应用到用户的杀毒软件的扫描引擎中。病毒特征的更新对于杀软的防护能力非常重要，图 6.3 给出了杀毒软件公司病毒特征的更新流程。图中根据病毒代码分析，找出核心运行特征，下发到用户杀毒软件中。

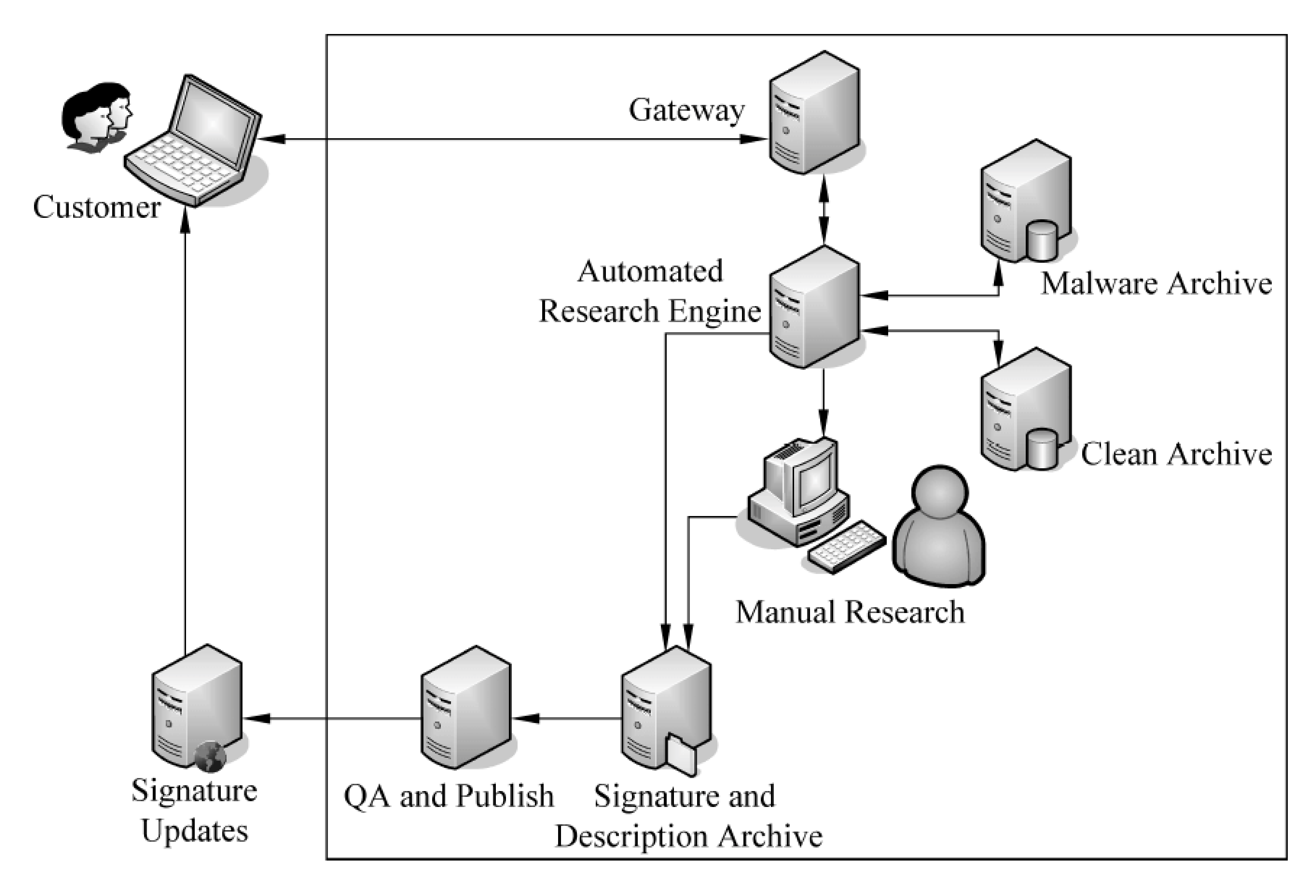


图 6.3　杀毒软件公司病毒特征更新流程

6.2.2 云查杀

云查杀(cloudscan 或 cloud-based scan)是通过客户端安全软件将可疑的病毒文件上传到云中心,在云中心汇总分析来判断病毒是否是恶意。云查杀大大降低了客户端的计算成本与开销,对于用户于预最少,而安全厂商借此广泛采集恶意软件样本,提高了响应应急的速度,因而是安全厂商大力推广的概念。典型的云查杀原理如图 6.4 所示。

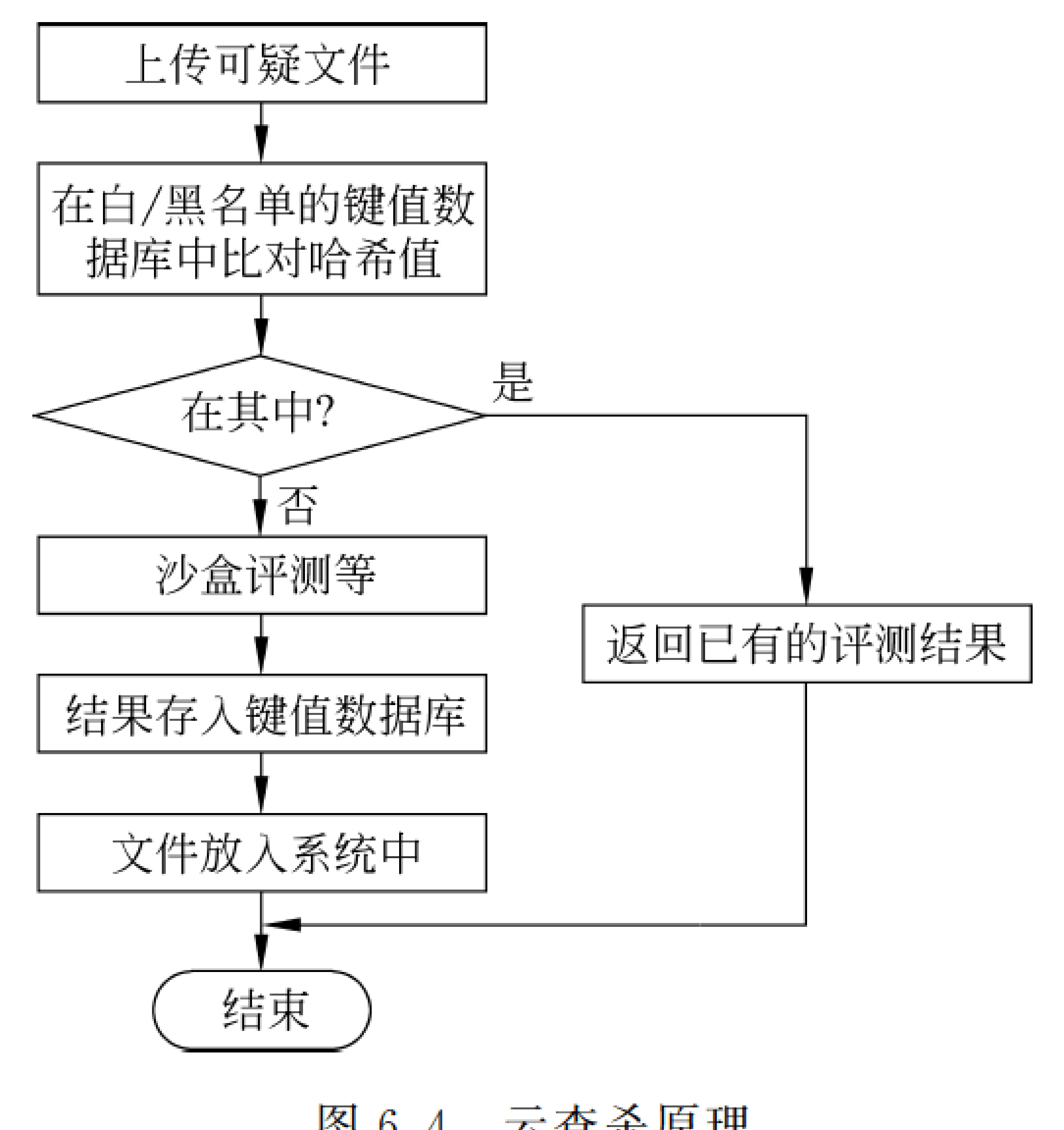


图 6.4 云查杀原理

恶意程序多是通过联网行为,将窃取用户的隐私发送至互联网特定主机上。安全卫士软件都拥有联网云查杀模块,通过上传用户设备上的可疑文件,在后端云服务器上进行分析,比对黑名单与白名单的海量应用的指纹。

安全卫士软件都有大量的联网行为,而软件的网络行为与用户安全息息相关,用户隐私与用户数据安全也面临空前挑战。

6.2.3 移动安全

随着安卓手机应用的流行,其安全问题也越来越严重。任何第三方都可以开发安卓应用软件并上传到应用市场,但各个应用市场的安全管理标准存在巨大差异。从应用市场上下载的应用软件也可以轻易地被篡改、添加恶意内容后重新上传到应用市场。与此同时,安卓的恶意软件和病毒程序开发成本低,Windows 上的病毒程序也可以轻松地移植到安卓中。这些因素都导致移动终端用户的安全,受到极大威胁。

移动设备由于能耗、计算和联网能力有限,在判断应用的性质上计算开销较高。面对如此海量的移动应用,只有通过云计算平台才能有效处理。MobSafe 系统云平台上,利用众多定制化的工具,来检测移动应用的安全性。MobSafe 系统自动化运行,对安卓应用进行分析。当一个 apk 文件提交到 MobSafe 进行分析时,它会首先检查在 key-value 存储的 redis 数据库中检查该 apk 文件是否已经分析,以及其结果是否已经存储在 Hadoop 的存储中。这种检查以 apk 文件的 hash 值作为 redis 键值存储的查询对象。如果查询成功,则把该结果返回;如果查询不匹配,则表明是一个新的 apk 文件。在这种情况下,该 apk 文件会被存储在 Hadoop 存储中。在此之后,一个守护进程将调用自动化分析工具,如 ASEF 和 SAFF,将分析结果和日志存储在指定的 Hadoop 目录下。与此同时,守护进程也会更新 redis 数据库与 Hadoop 的存储结果目录。经过这段时间的分析处理之后,再把分析结果返回给用户。

Mobsafe 的 Web 前端基于 SpringSource 的 Spring 框架和 Twitter 的 Boostrap 框架开发。它提供了可疑安卓应用的上传功能，并且把后台返回的分析结果在网页中展示。Mobsafe 的后台利用了一系列分析工具，进行深入检测。下面介绍安卓应用安全分析的两个主要框架。

其中 ASEF(Android Security Evaluation Framework)是一个自动化的工具，用于分析 Android 应用。当提交一个未知的 apk 文件到 ASEF 进行分析时，首先它会启动 ADB 记录日志和 TCPDUMP 进行流量嗅探，然后启动一个 Android 虚拟机(AVD)并把该 apk 安装进去。之后，ASEF 开始启动应用程序进行分析，并发送一些随机的手势来模拟用户的操作。把一定次数的手势发送到虚拟机之后，测试流程结束，该应用程序被卸载。然后 ASEF 将开始分析日志文件和应用程序产生的上网流量。ASEF 使用谷歌公司的安全浏览 API 来找出应用程序访问的 URL 是否为恶意链接。ASEF 还检查已知的漏洞列表，找出该应用程序是否存在一些严重的漏洞。

SAAF(Static Android Analysis Framework)是一个 Android apk 文件的静态分析工具。它可以提取 apk 文件的内容，将其解码为 smali 代码，然后使用应用程序切片分析方式来分析 smali 代码，进行应用程序权限分析，启发式模式匹配，并对感兴趣的函数进行切片分析。

此外，Mobsafe 还利用了众多静态分析工具，如 readelf、ded、apktool、androguard 和 soot 等，这些工具大都基于逆向工程。还有一些动态分析工具，如 Strace 和 randoop 等，用来分析应用程序运行时的行为，Strace 用来记录 Linux 内核的系统调用，randoop 用来给应用程序一些随机输入并记录其输出。

6.3 网络侧的防护

基于网络的安全攻击越来越高级，手段和模式不断演进，在网络侧的防护主要问题如图 6.5 所示，主要包括 3 方面。

① 攻击模式变换，模式越来越多，如何实时过滤网流内容，阻止安全攻击?

② 攻击手段升级，通过扰乱网包次序，意图逃避安全检查和内容过滤，如何防御?

③ 新型未知攻击，尚未有检查手段，如何有效归档网流，追踪还原事发现场?

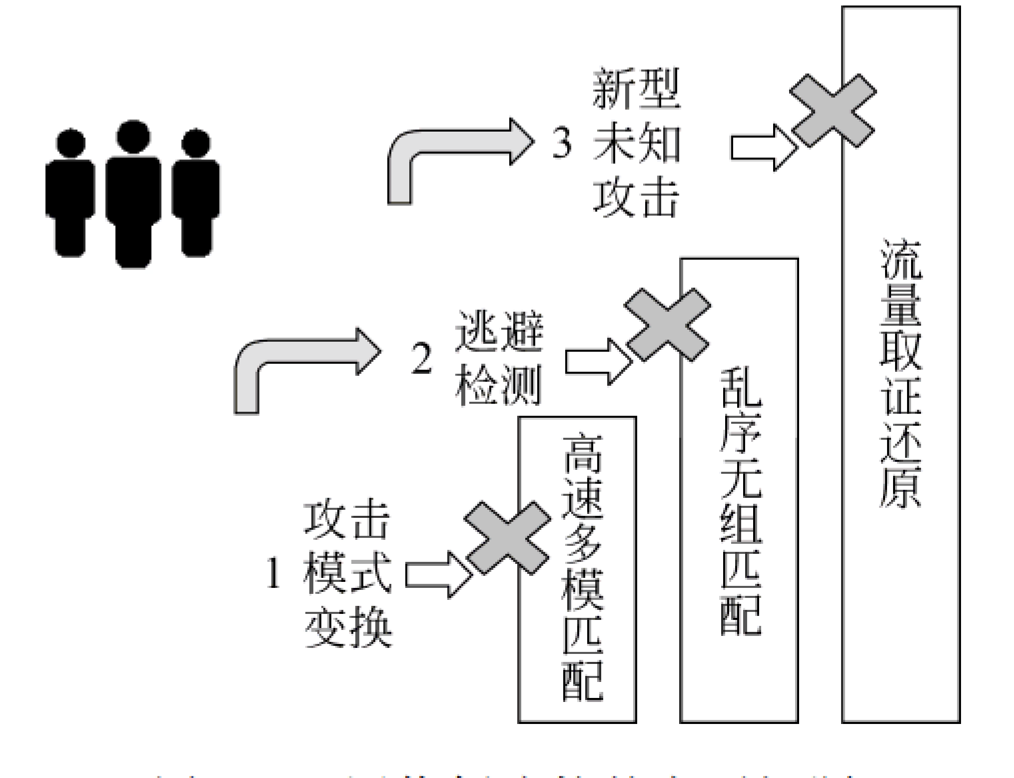


图 6.5 网络侧防护的主要问题

6.3.1 防火墙

防火墙(FireWall)是介于其他网络和防火墙所保护的网络之间的中界点，控制被保护网络和其他网络之间的数据包交换的网络设备。RFC 2979 定义了防火墙的行为和需求，基于以上规范的软件或是硬件，称为防火墙，如图 6.6 所示。

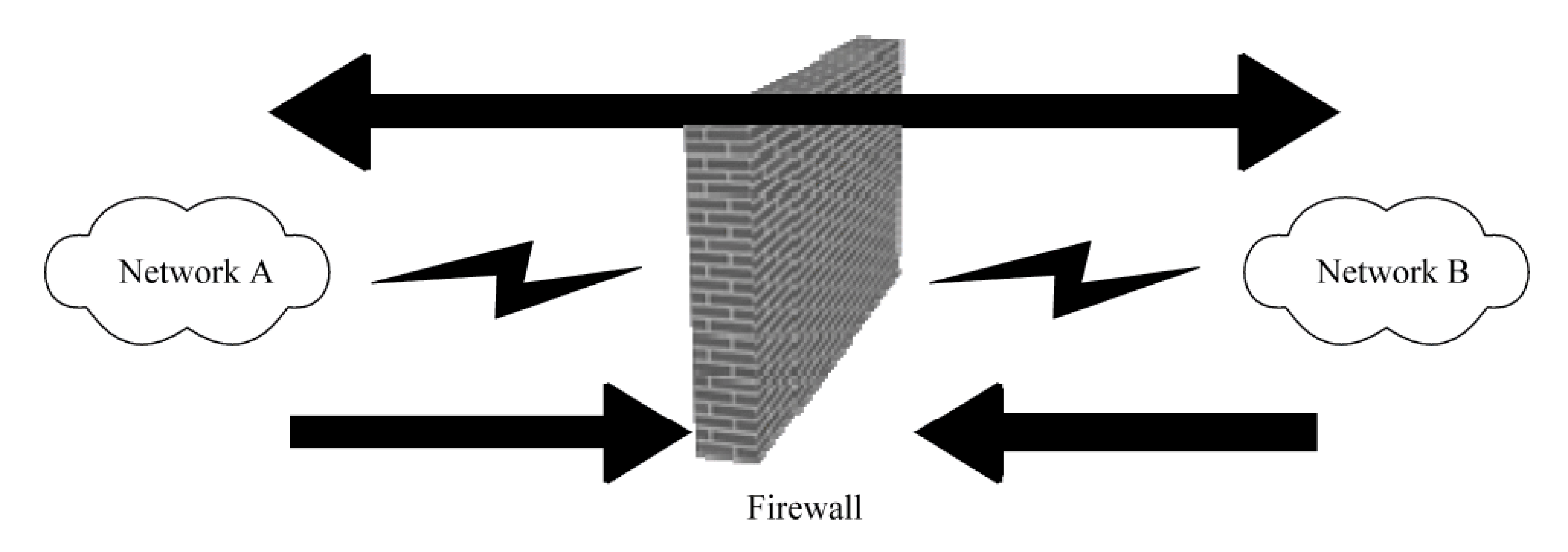


图 6.6　防火墙基本原理

防火墙能够防止未经允许的连接进入由防火墙所保护的网络,防火墙提供了穿透(Transparency)的功能,并提供了限制穿透的功能。

性能较好的是基于硬件 ASIC 或多核网络处理器的防火墙,如启明星辰、绿盟 NF 万兆防火墙系列。

目前主机防火墙也日益普遍,如 Windows 自带防火墙、Norton Internet Security、瑞星个人防火墙等。

6.3.2　入侵检测系统

入侵检测/阻止系统(Intrusion Detection/Prevention System)是对网络流量内部的数据进行深入检测(Deep Packet Inspection,DPI),根据已有的攻击特征和模式,实时检测或者阻止匹配的攻击。IDS/IPS 会有一定的误判率(False Positive),即把不是攻击的正常流量误报为攻击流量。

入侵检测系统(Intrusion Detection System,IDS)监控网络中恶意的行为并进行报警。当检测到攻击时,它可以丢弃异常的网包同时允许所有其他流量通过。入侵检测系统则运行在旁路模式,即只有报警功能,没有阻断功能。与之相对应的是入侵防御系统(Intrusion Prevention System,IPS),该系统运行在在线模式,可以随时进行阻断。

1. Snort

Snort 最初由 Martin Roesch 开发,它是目前使用最广的开源入侵检测系统项目,规则集比较丰富,目前最新的稳定版本为 2.9.7。很多商业的入侵检测系统也采用 Snort 系统。它可以实现实时的流量分析和网包记录,其功能包括协议分析、内容匹配,以及探测诸如内存溢出、端口扫描、CGI 攻击、SMB 探测、OS 识别等攻击。Snort 的检测机制属于特征匹配,即针对每一种攻击,都提取出一种特征来定义它,从而形成一套规则集(Rule Set)。运行时,从网络中捕获网包,并和载入的规则文件中的特征进行对比,若有匹配则认为出现入侵,从而报警并记录。

2. Bro

Bro 入侵检测系统是加州大学 Berkeley 分校的 Vern Paxson 教授开发的入侵检测

系统。Bro 提供 broccoli 接口，可以进行协同。另外，Bro 也提供流量 DPI 功能，检测不同协议的攻击。可访问 www. bro-ids. org，以了解更多信息。

3．pfsense

pfsense 是基于 FreeBSD 的流量管理控制软件。pfsense 项目由 BSD perimeter LLC 公司推出，该项目启动于 2004 年，是 m0n0wall 的克隆项目，它包含所有商业防火墙和 UTM 的功能。pfsense 是基于 FreeBSD 8.1 的软路由服务器平台软件，于 2006 年 2 月发布版本 1.0，目前版本为 2.1.5。可访问 www. pfsense. org，以了解更多信息。

6.3.3　蜜罐网络

蜜罐（Honeypot）是指伪装的不安全计算机系统，用于吸引攻击、观察攻击的网络工具。蜜罐网络（Honeynet）是用多个蜜罐组合起来的网络系统，用来采集攻击者的信息，进而掌握攻击者的行为规律，从而为人们更好地维护网络、保护计算机系统的安全性提供支持。

蜜罐网络的关键技术有网络虚拟化、端口重定向、报警、数据控制和数据捕获等。一般实验采用虚拟机（VM）虚拟出蜜罐网络，其中有防火墙、入侵检测系统和多个服务器。

加州大学 Berkeley 分校的 Vern Paxson 教授组建的 GQ 蠕虫分析系统就是一个类似蜜罐网络分析系统，通过从互联网采集目的地址无应答的流量（疑似蠕虫流量），将该流量重放（Replay）到蜜罐网络系统，观察其流量引发的连锁反应，以确定是否为蠕虫流量，如图 6.7 所示。

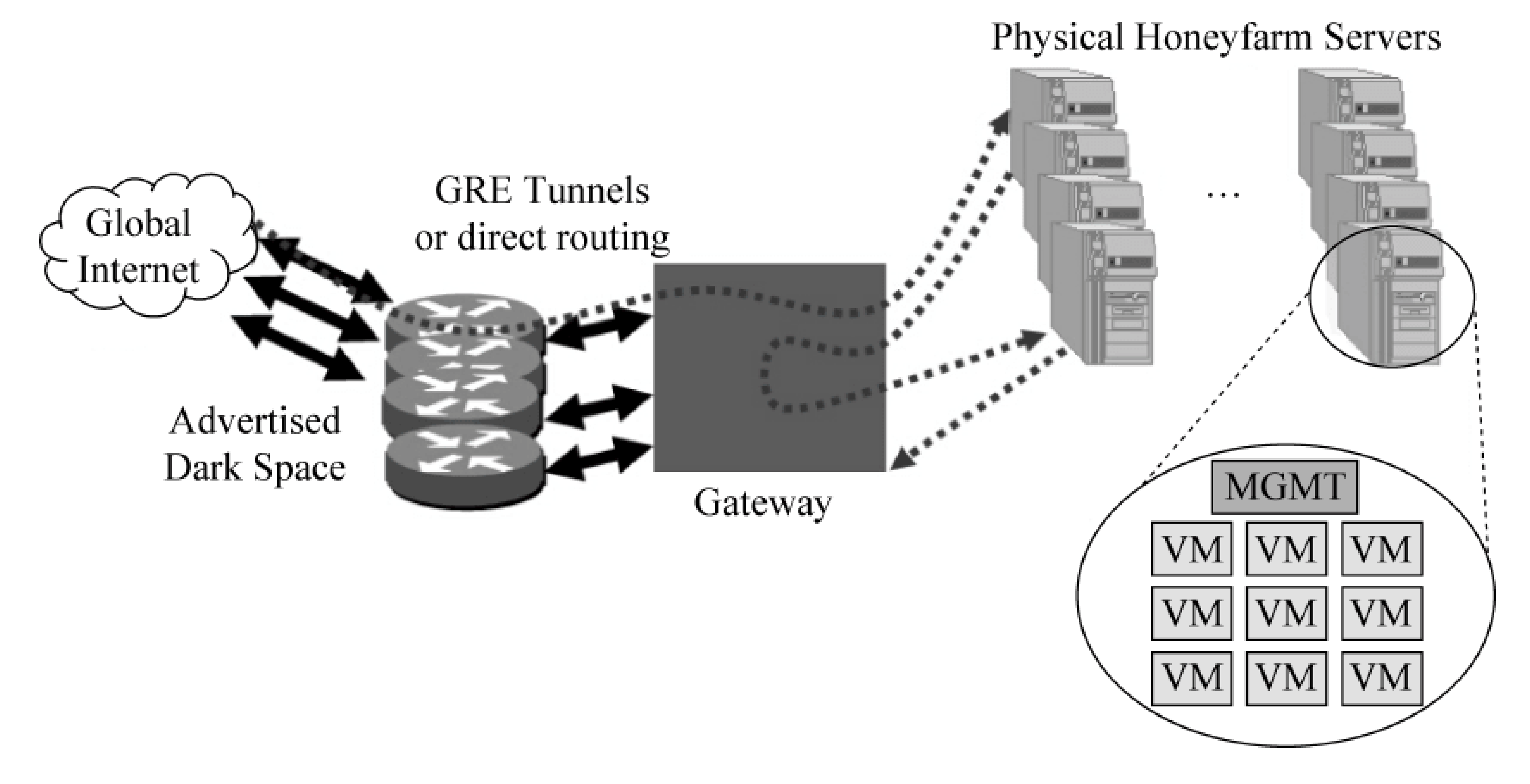


图 6.7　GQ 蠕虫分析系统

解决问题有多种途径，除了直接硬碰硬外，还可以以退为进，在互联网的世界安全里这个策略依然适用。蜜罐技术就是这样的防护技术。

6.3.4 流量归档分析

该系统为处理海量流数据设计，包括流数据的记录、归档、索引、查询、挖掘功能，能应用于传感器、探针、监视器采集流数据的处理，具有较大的应用价值。

在网络流数据处理中，网络安全事件（如钓鱼网站等）需要取证研究。通过与 UTM 设备配合使用或者作为 UTM 的一个功能模块，实现网络安全事件取证。在 UTM 中整合了 Time Machine 和 FastBit，采用 Time Machine 实现流量获取与记录功能，采用 FastBit 实现流量记录索引与查询功能，利用 htop 工具给出图形化显示界面。

1. 主要特性

（1）大存储。实现了多块大容量硬盘的轮流存储。

（2）易查询。用户可以便捷地进行查询。

（3）高性能。查询响应迅速，对于 100 万个数据包的原始记录，在 10min 内建立索引，在 1min 内响应查询请求。

2. 主要功能

（1）实现流量实时存储，实现基于 IP-SAN 的外置存储，经 iSCSI 协议与 CTM 实现数据传输。

（2）实现连续 90 天（3 个月）的流量记录存储，可查询最近 90 天（3 个月）的流量存储。

（3）默认为 12TB 存储容量，最高支持 24TB～180TB(需多台存储服务器和万兆交换机）存储流量。

（4）可实现基于时间和日期、IP、流量内容等的查询。

6.3.5 DDoS 对抗

在大规模网络服务中一般都会部署 Snort 入侵检测系统，通过 Snort 监控出入流量，万兆 Snort 入侵检测系统部署方案如图 6.8 所示。实现功能有万兆级网包获取、网流的大数据存储与计算、多数据中心汇聚，通过 TCP 协议 RST 信号实现旁路阻断等。

Web 服务前端一般都会部署 Web 应用防火墙 WAF，通过 WAF 监控出入 Web 的流量，对 Web 攻击识别与旁路阻断。旁路 Web 实时监测系统用于检测可能的 Web 安全攻击。这些监测数据总是不断地产生，需要根据当前的监测数据实时做出是否存在 DDos 攻击判断，因此流式计算（Stream Computing）用来解决大数据的时效处理。

在监测数据实时采集方面，完整地收集到所有安全设备的日志数据，为实时应用提供实时数据。目前，日志数据采集工具有 Scribe、Kafka、Flume、TimeTunnel 和 Chukwa 等，它们均可以满足每秒数百兆字节的日志数据采集和传输需求。

对于流式处理，目前常见流式计算系统有 Twitter Storm 和 Yahoo！S4。其他高效处理平台还有 Facebook Puma3 和 Apache Spark 等。

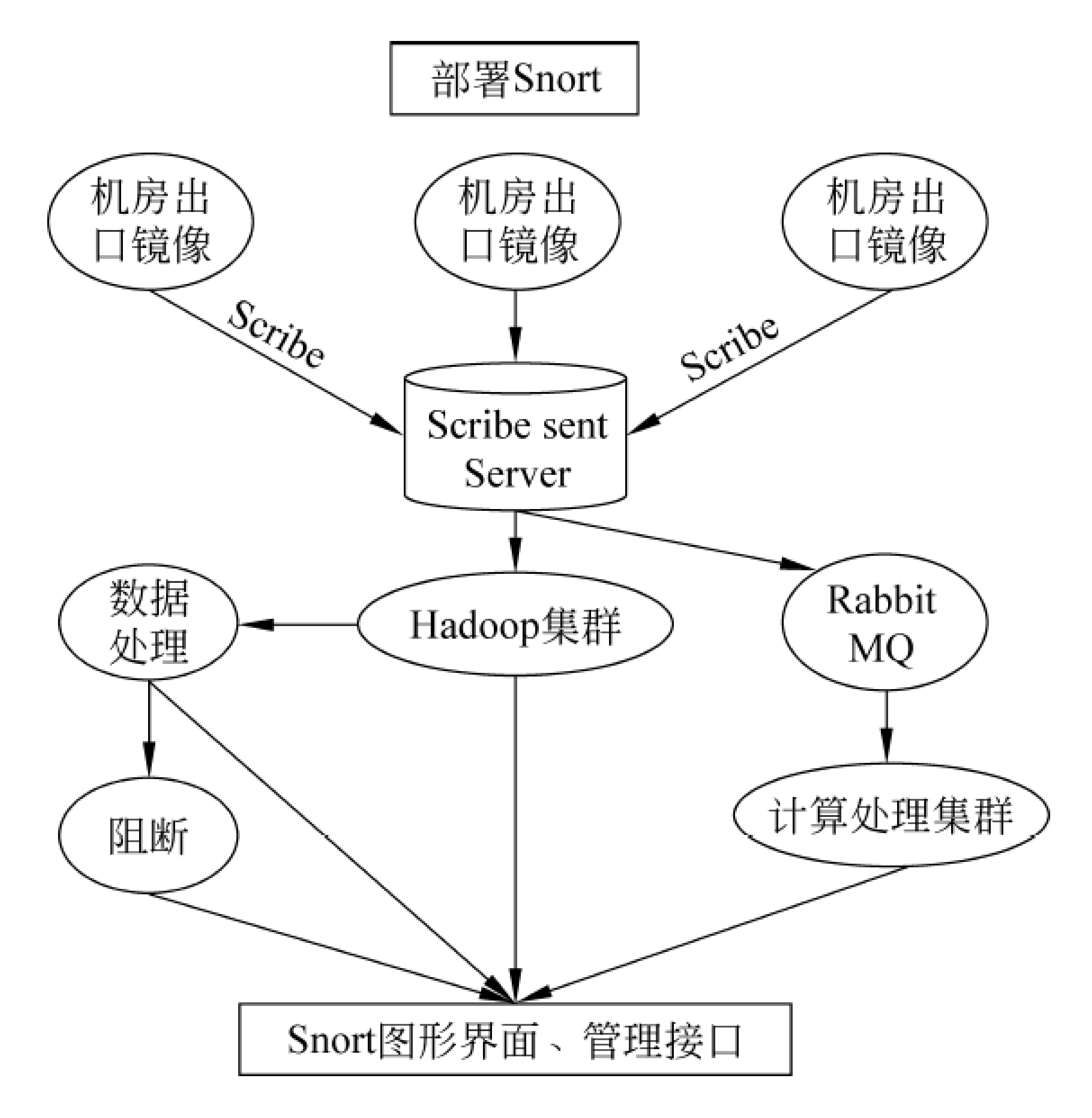


图 6.8　万兆 Snort 入侵检测系统

第 7 章　通信安全与密码学

7.1　通信安全需求

通信安全是指在通信场景下,保护交互双方的信息交互的机密性、完整性、可认证性。信息加密的基本思想是通过变换信息的表示形式来伪装需要保护的敏感信息。网络安全使用密码学来辅助完成在传递敏感信息的相关问题。密码是通信双方按约定的法则进行信息特殊变换达到伪装保护敏感信息的一种重要保密手段。密码学的首要目的是隐藏信息的含义,并不是隐藏信息的存在。

互联网中的通信,是在不可靠网络的可靠通信,缺乏信任环境下的安全通信。举一个典型通信场景:爱丽丝(Alice,简称 A)想和她的存款银行 Bank(B)进行一些金融事务过程,Eve 是潜在具备发动的中间人攻击的第三方,如图 7.1 所示。在这种情况下,通信安全基本要求包括机密性(Confidentiality)、完整性(Integrity)以及可认证性(Authentication)。

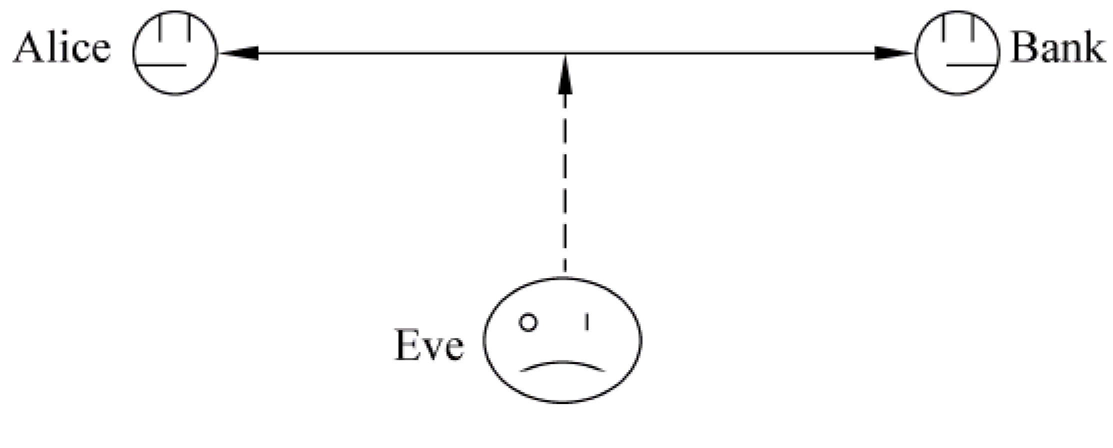


图 7.1　中间人攻击

1. 通信的机密性

不应出现未经授权的 Alice 信息的公开,除了 Alice(A)和银行 Bank(B),其他任何人不应该获悉她们之间的信息交换内容。

2. 通信的完整性

不应出现未经授权的信息操作,除了 Alice(A)和银行 Bank(B),其他任何人不应该能够修改她们之间的信息交换内容。

3. 通信的可认证性

接收者 Bank(B)应该能够确认信息的起源的能力。入侵者不应能够伪装其他用户,如 Alice(A)。

简单地讲,机密性是指密文内容无法被他人轻易读取;完整性是指当数据出现脱漏或被人为修改时,它可以被发现甚至修复;可认证性是指信息的发出者身份可以被接收者确认,避免冒用身份。如何满足信息通信安全需要,特别是信息安全的机密性、完整性和可认证性(CIA 特性),需要密码学的知识和工具。

密码学的 3 种手段主要是对称密码学(Symmetric Cryptography)、密码哈希函数(Crypto Hash Function)以及公钥密码学(Public Key Cryptography)。

7.2 密码学概论

本节介绍密码学的基本概念和常识,着重介绍基于对称密码、非对称密码、密码哈希函数,并通过一个比特币等数字货币的设计和实现过程来说明如何应用密码学。

密码学的基本工具包括加解密算法、密码哈希函数、签名与验证。从体系规范的角度来看,分为对称密码体制和公钥密码体制。密码协议的发展和密钥管理与分发的健全促进了密码学向自动化方向发展。

密码学是理论计算机科学的重要内容,是计算理论、信息论和数论的交叉学科,如图 7.2 所示。寻找某些计算困难的问题的,一直是密码学的基础。如何衡量一个问题的计算难度是计算复杂性的问题。加密的核心就是算法,通过密钥将明文转化成密文。与之相对的是解密,即从密文恢复出明文。图 7.3 给出了密码学与算法的关系。

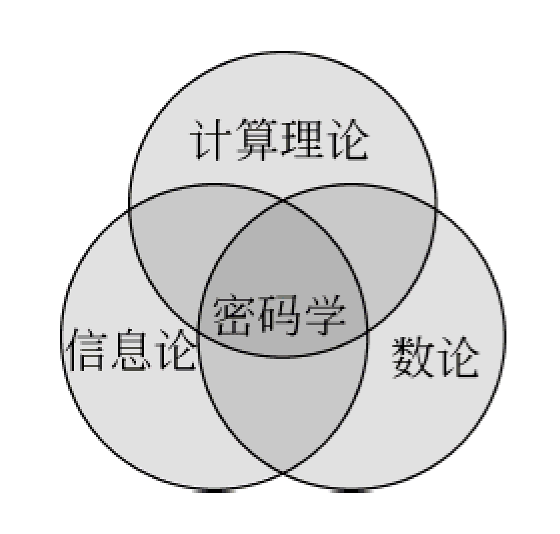


图 7.2 密码学是一个交叉学科

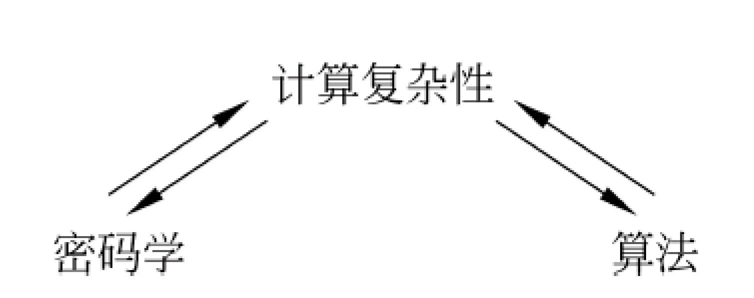


图 7.3 密码学与算法的关系

2002 年美国计算机学会的图灵奖颁给了麻省理工学院(MIT)的 Ronald L. Rivest Adi Shamir 和 Leonard M. Adleman,以表彰他们提出了 RSA 公钥密码算法。2012 年美国计算机学会的图灵奖又颁给了麻省理工学院(MIT)的 Shafi Goldwasser 和 Silvio Micali 教授,以表彰他们对基于复杂理论的密码学的数学可证明性的贡献。

密码学包括密码编码学和密码分析学。密码学是一种非常有趣的学科,体现了对立与统一,它分为密码编码和密码分析,可以说是矛与盾的关系。

编码学研究对信息进行编码,实现信息隐藏,研究与信息安全(机密性、完整性、可认证性)有关的数学技术,包含数据变换的原理、工具和方法,目的是为了隐藏数据的信息内容,防止篡改数据及未经认可使用数据。

密码分析学研究加密消息的破译或消息的仿造,针对编码技术及信息安全服务做破解。分析密码体制的输入输出关系,找到机密信息对应的明文或者是密钥等敏感

信息。

7.2.1 密码工具标准

密码学手段和工具包括加解密算法、密码哈希函数、签名与验证、密码协议等。在这些基本密码工具的基础上，架构对称密码体制、公钥密码体制、安全哈希函数和密钥管理与分发。在此基础上，并最终标准化形成了现在网络环境下的信任机制 PKI 框架和 X.509 证书系统。

基于 PKI 框架和 X.509 证书是目前政府及商业网站防止被钓鱼和假冒的基本技术手段，也是互联网内容安全的基础。图 7.4 给出了美国标准技术局(NIST)制定的密码学标准及其分类。主要内容包括对称密钥算法、公钥算法、安全哈希和随机数生成。

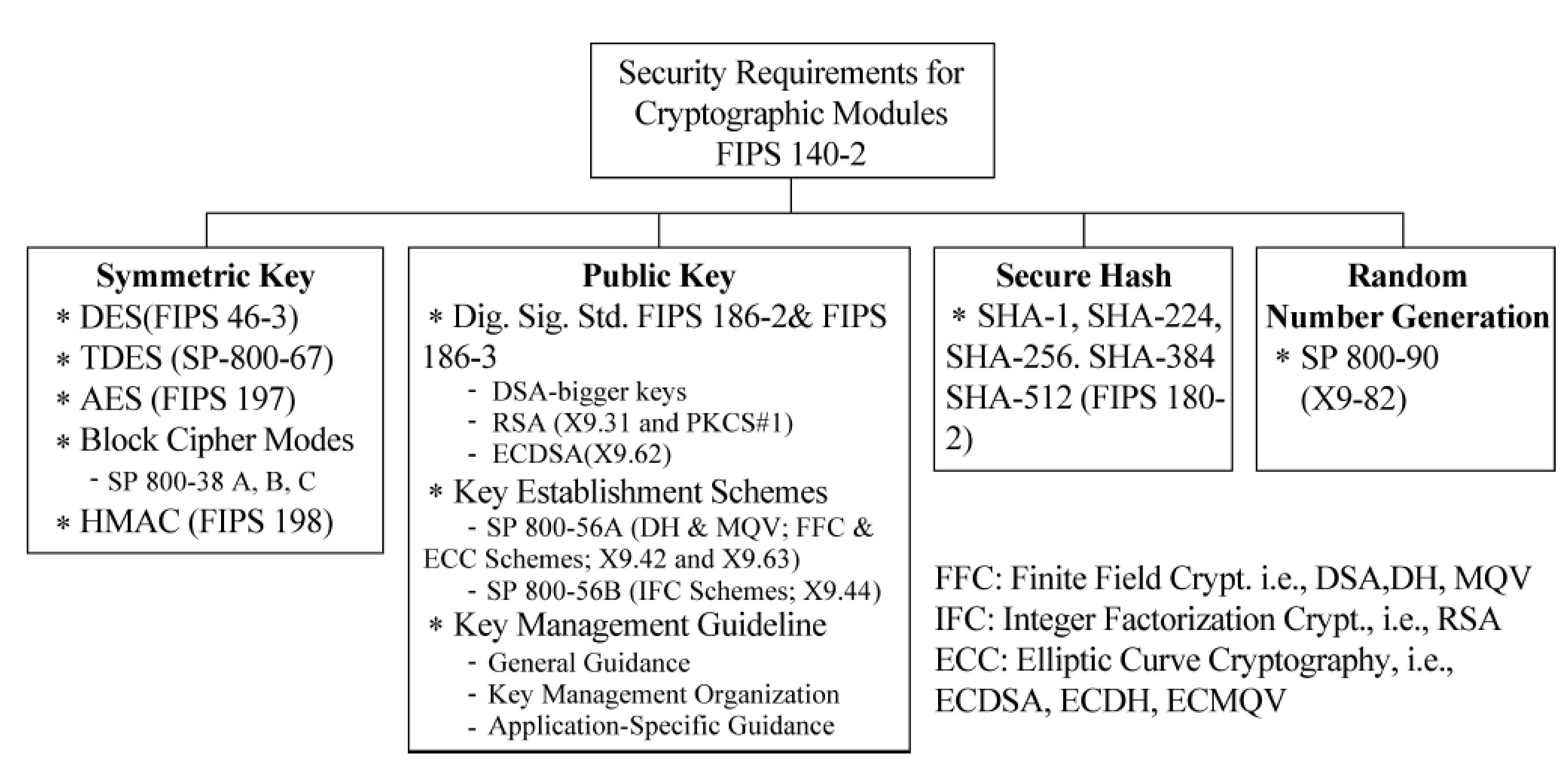


图 7.4 密码学标准及其分类

我国商用密码标准主要有 SM2 公钥密码算法、SM3 密码哈希函数和 SM4 分组加密算法。SM2 椭圆曲线密码算法包括 3 个子算法：椭圆曲线数字签名算法(SM2-1)、椭圆曲线密钥交换协议(SM2-2)、椭圆曲线公钥加密算法(SM2-3)。另外，在 3GPP 无线标准上提出了祖冲之流密码算法(ZUC)，引起人们极大关注。

7.2.2 密码管理政策

密码学的 Kerckhoff 原理指出，对任何一种攻击方法，都假定密码分析者事先知道所使用的密码体制，那么，密码系统的安全性完全取决于密钥中。密码分析者知道双方使用的密码系统：明文的统计特性及加解密体制。

根据研究应用的对象不同，密码管理策略也不同。

密码研究者和私营部门的一些算法是公开的，其安全性取决于密钥，这种方式可以经受公众的挑战，类似于开源软件的方式，有利于改进算法，如 3GPP 无线加密算法/祖冲之算法便是其中之一。

军事部门和政府的密码算法是国家机密，一般不公开，其安全性取决于算法和密

钥。这种方式主要是利用信息的不对称，保护自身算法，例如各国有严格的密码管理策略用以限制密码出口，对外国算法研究进行限制。

7.2.3 加密算法设计原则

密码学中最重要的是加密过程。密码加密算法的设计方法主要通过信息的混淆(Confusion)和扩散(Diffusion)两种方法。

“好”的加密算法应该具备“非线性原则”和“雪崩原则”。“非线性原则”指输出不应该是输入的线性变换，确保混淆效应；“雪崩原则”指输入的任何集合改变，输出的任意比特被改变的概率是 0.5，确保扩散效应。

如果加密前的输入和加密后的输出成线性关系的话，攻击者就能很容易地推出整个变换过程，通过“非线性原则”就保证了混淆性质。为了防止黑客通过逐一改变微小的输入来监测输出从而猜测出算法，就必须要求输入集合的微小改变就要导致输出的巨大变化，“雪崩原则”就保证了这一扩散性质。

直观上想，若是线性变换，加密是很容易破解出来的。反之，若不是线性变换，要怎样的加密才最可靠呢？原文的任意一处改动，密文的每一处都有可能会随机改变加密，这样才最不易破解。

任何密码的安全都是相对的，最坏情况取决于暴力破解的难度，即穷举密钥的所有的可能性。而超级计算机的计算能力事实上意味着暴力破解密码的能力。这也解释了世界各国不断研制更强大的超级计算机的动力。

中国在密码学方面也做出了不少贡献，例如，上海交通大学的来学嘉教授和梅西教授设计的 IDEA 加密算法，至今一直为 PGP(Web of Trust)使用。2004 年山东大学的王小云教授破解了 MD5 哈希函数，接着又攻破了 SHA-1 哈希函数，从而推动美国国家标准技术局 NIST 于 2008 年开始，进行新一轮的哈希函数竞赛，以代替 MD5 和 SHA-1 函数。2012 年 10 月，NIST 正式宣布 Keccak 算法为 SHA-3 标准，Keccak 算法为比利时的研究组(Guido Bertoni，Joan Daemen，Michaël Peeters，Gilles Van Assche)提出。对 SHA-3 的破解又将成为研究的一个新热点。

7.3 密码学基础

7.3.1 密码系统

密码系统是一个五元组(P,C,K,E,D)，其中，P 是明文空间，C 是密文空间，K 是密钥空间，E 是加密算法空间，D 是解密算法空间，其流程如图 7.5 所示。

$\forall k\in K$，$\exists$ 加密算法 $e_k\in E$，相应的解密算法 $d_k\in D$，S. t. 加密函数 $e_k:P\rightarrow C$，解密函数 $d_k:C\rightarrow P$，满足 $d_k(e_k(x))=x$，这里 $x\in P$。

密码系统是保障安全通信的系统，而密码学是密码系统的关键理论与技术。

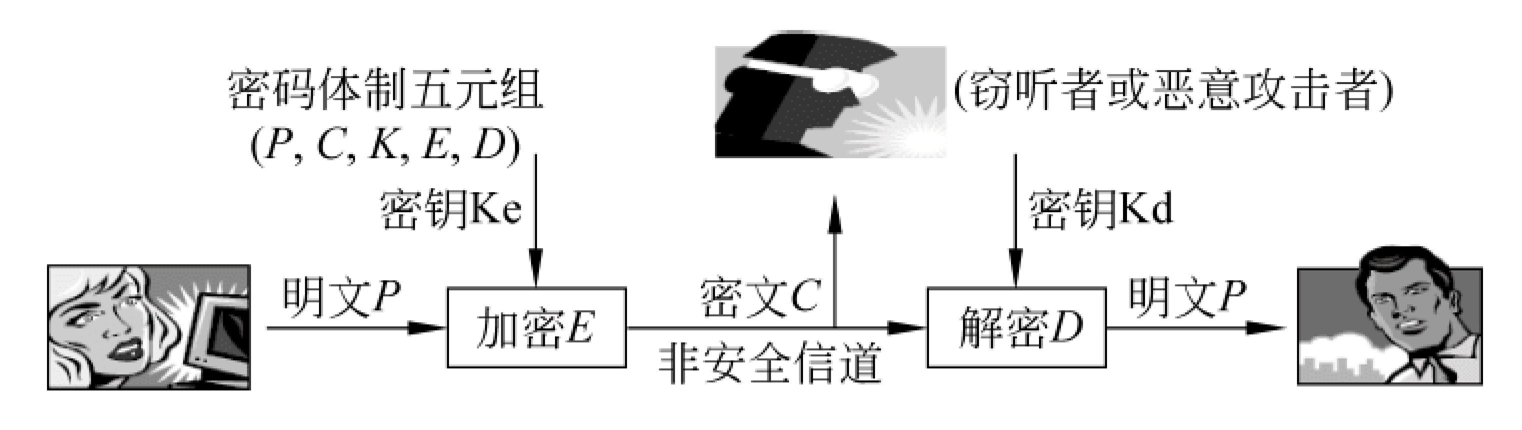


图 7.5　密码学基本流程

7.3.2　密码学历史

1. 古典密码(古代至 19 世纪末)

古典密码主要是代替密码(substion code)和换位密码(permutation code),如凯撒密码、维吉尼亚密码、栅栏密码等。凯撒密码的基本思想是通过把字母移动一定的位数来实现加密和解密。明文中的所有字母都在字母表上向后(或向前)按照一个固定数目进行偏移后被替换成密文。例如,当偏移量是 3 的时候,所有的字母 A 将被替换成 D,B 变成 E,以此类推,X 将变成 A,Y 变成 B,Z 变成 C。由此可见,位数就是凯撒密码加密和解密的密钥。

维吉尼亚密码是在凯撒密码的基础上扩展出来的多表密码,由 16 世纪法国亨利三世王朝的布莱瑟·维吉尼亚发明,其特点是将 26 个凯撒密表合成一个表,同时引入了“密钥”的概念,即根据密钥来决定用哪一行的密表来进行替换,以此来对抗英语中字频统计。

2. 近代密码(20 世纪初至 1949 年)

密码学发展到近代,出现了机械/机电方式的自动化密码技术,如 Engima 加密机、洛伦兹加密机等。

Enigma 读作“恩尼格玛”,其结构如图 7.6 所示,它为第二次世界大战中德国方面所使用,意为“谜”。由 1918 年德国发明家亚瑟·谢尔比乌斯(Arthur Scherbius)和他的朋友理查德·里特(Richard Ritter)联合发明。Engima 加密机将密码技术从手工时代带入了电气时代。而在线密码电传机洛伦兹加密机(LorenzSZ 42),大约在 1943 年由 Lorenz A.G 制造。英国人称其为 tunny,用于德国战略级陆军司令部。

3. 现代密码(1949 年至今)

克劳德·香农(Claude Shannon)于 1949 年发表了论文 *The Communication Theory of Secret Systems*,奠定了现代密码学的信息论基础,并提出了加密解密算法的设计。

7.3.3　对称加密算法

对称加密算法是应用较早的加密算法,技术成熟。加解密密钥都是相同的,保密性依赖于密钥。

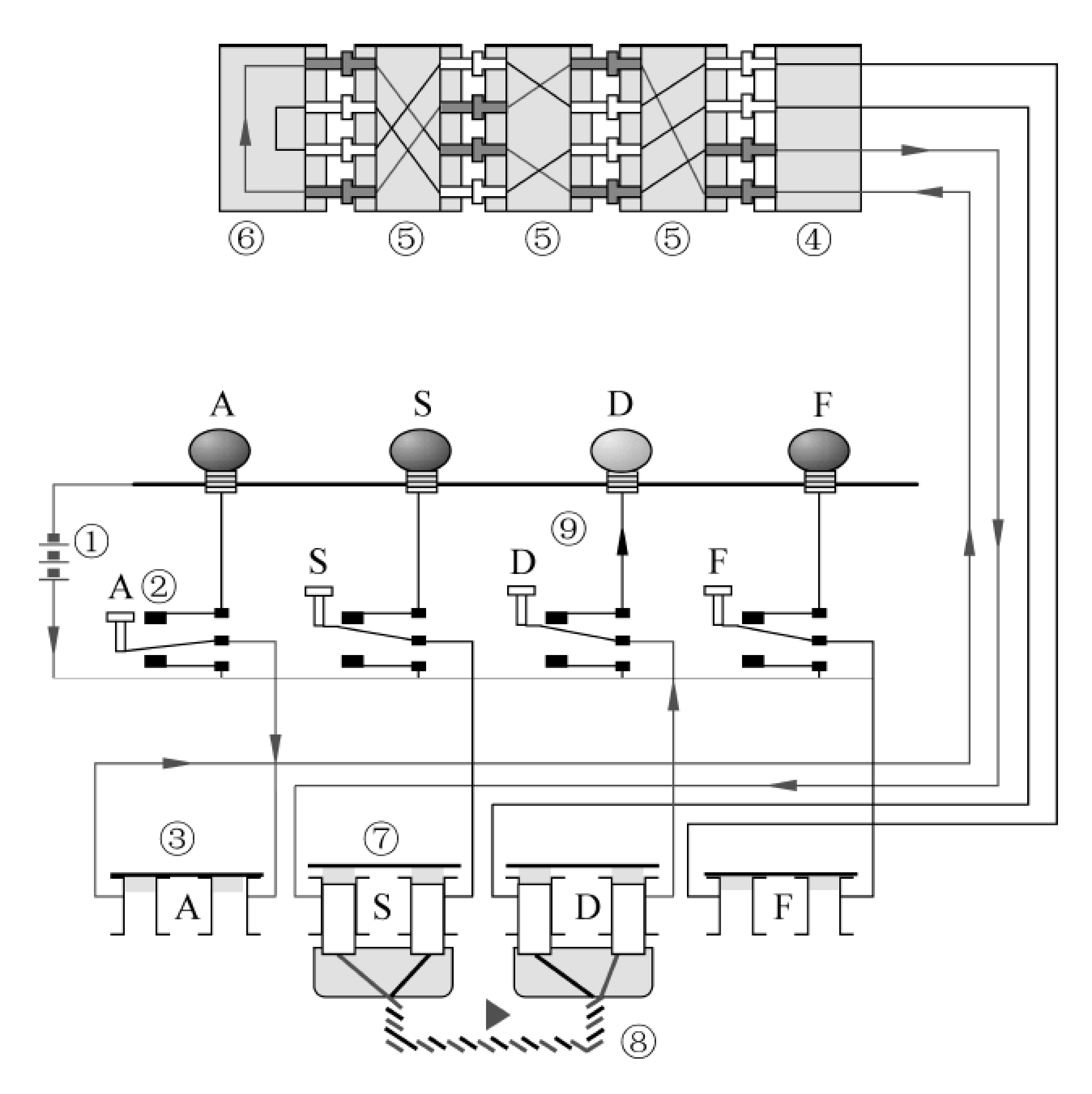


图 7.6　恩尼格码加密机

1. 替换置换网络

香农于 1949 年提出替换置换网络(Substitution-Permutation networks),简称 S-P 网络。S-P 网络采用两种基本密码操作:S-box 和 P-box,提供对明文的混淆和扩散操作。

2. Feistel 结构

Feistel 结构应用很广,是分组密码的基础部件。Feistel 结构 20 世纪 70 年代由 Horst Feistel 发明,如图 7.7 所示。

基于 Feistel 结构的对称加密算法构建的过程如下:通过 S-Box 和 P-Box 两者的基础结构来对原信息进行替换和打乱,以得到加密效果。同时借助异或运算的可逆性,使得解密仅需简单的反着加密的过程进行即可。

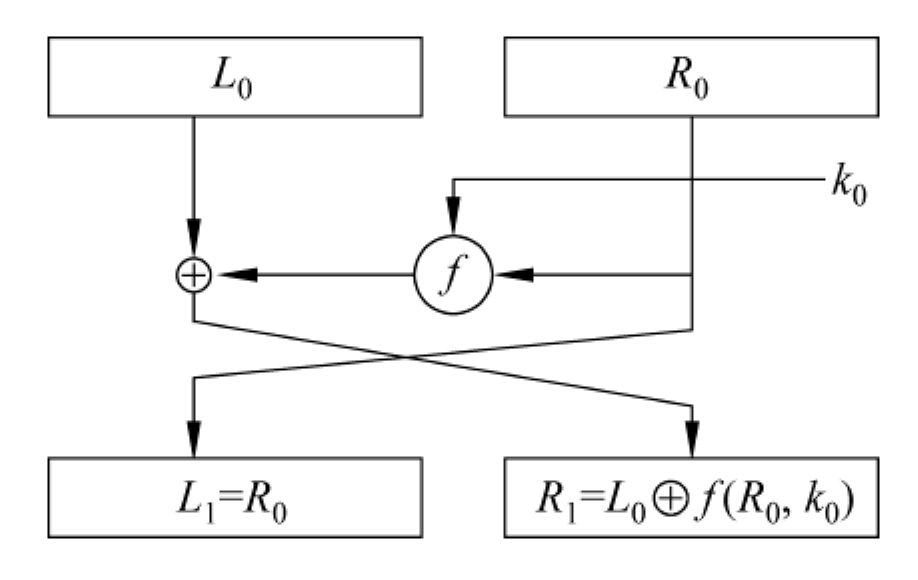


图 7.7　基本 Feistel 结构加图号

Feistel 结构类似于平时的洗牌方法,这个加密的方法把数据分在左右边,其中一边通过 f 函数操作一次后,两边互换,重复之前的操作,如此进行完成加密,反过来则是解密的过程。

Feistel 结构使得加密机和解密机合二为一,加密反过来就可以解密,算法还可以通过换机器部件来做到时刻改变,既增加了方便性,又提高了安全性。

1) DES 数字加密标准

DES(Data Encryption Standard)为美国国家标准局 NIST 于 1977 年公布的由

IBM 公司研制的一种加密算法,批准为非机要部门使用的数据加密标准。

DES 加密标准是使用 16 轮 Feistel 结构的加密算法,如图 7.8 所示。其优点有:加密与解密可以由相同的设备完成,通过采用不同的 S-Box 可以配置给不同的部门使用,其结构采用相同的 Feistel 结构接连而成,便于维修与维护。

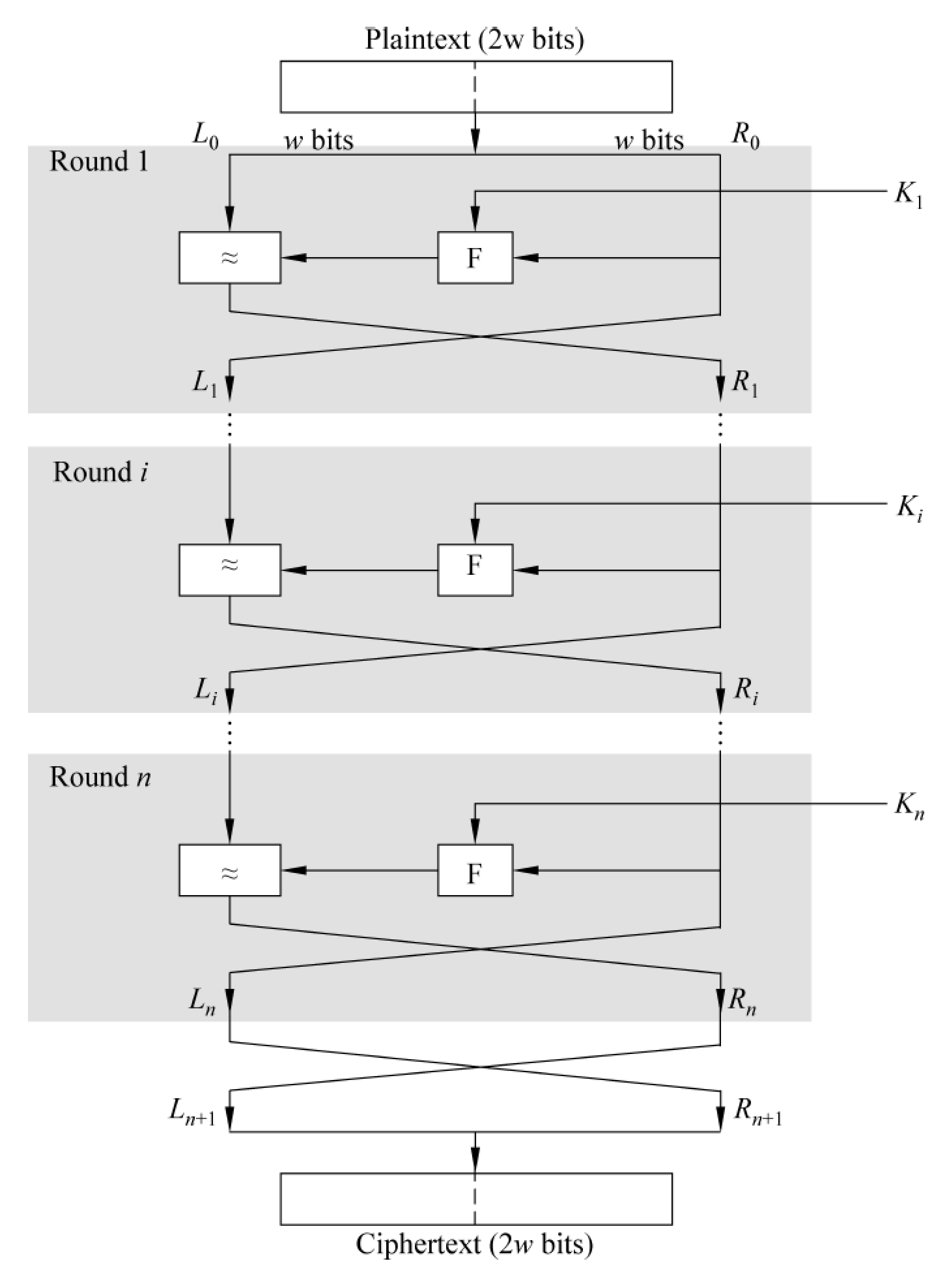


图 7.8　DES 加密算法

2）AES 高级加密标准

美国国家标准局于 1997 年开始确定一个全球免费使用的分组密码,1998 年公布了 15 个 AES 候选算法,2000 年公布了 5 个 AES ,即 Rijndael、MARS、RC6、SERPENT、TWOFISH,然后从这 5 个中选出一个。最终,比利时的 Joan Daeman 和 Vincent Rijmen 提交的算法 Rijndael 获选。AES 加密算法如图 7.9 所示。

7.3.4　公钥密码

1976 年,美国斯坦福大学的 Diffie 和 Hellman 发表 *New Directions in Cryptography*。在公钥密码学中公开密钥和私有密钥成对出现且互不相同,私有密钥不能根据公开密钥计算出来。公开密钥 k_1,可以公开,即任何人能用公开密钥加密信息,但只有相应的

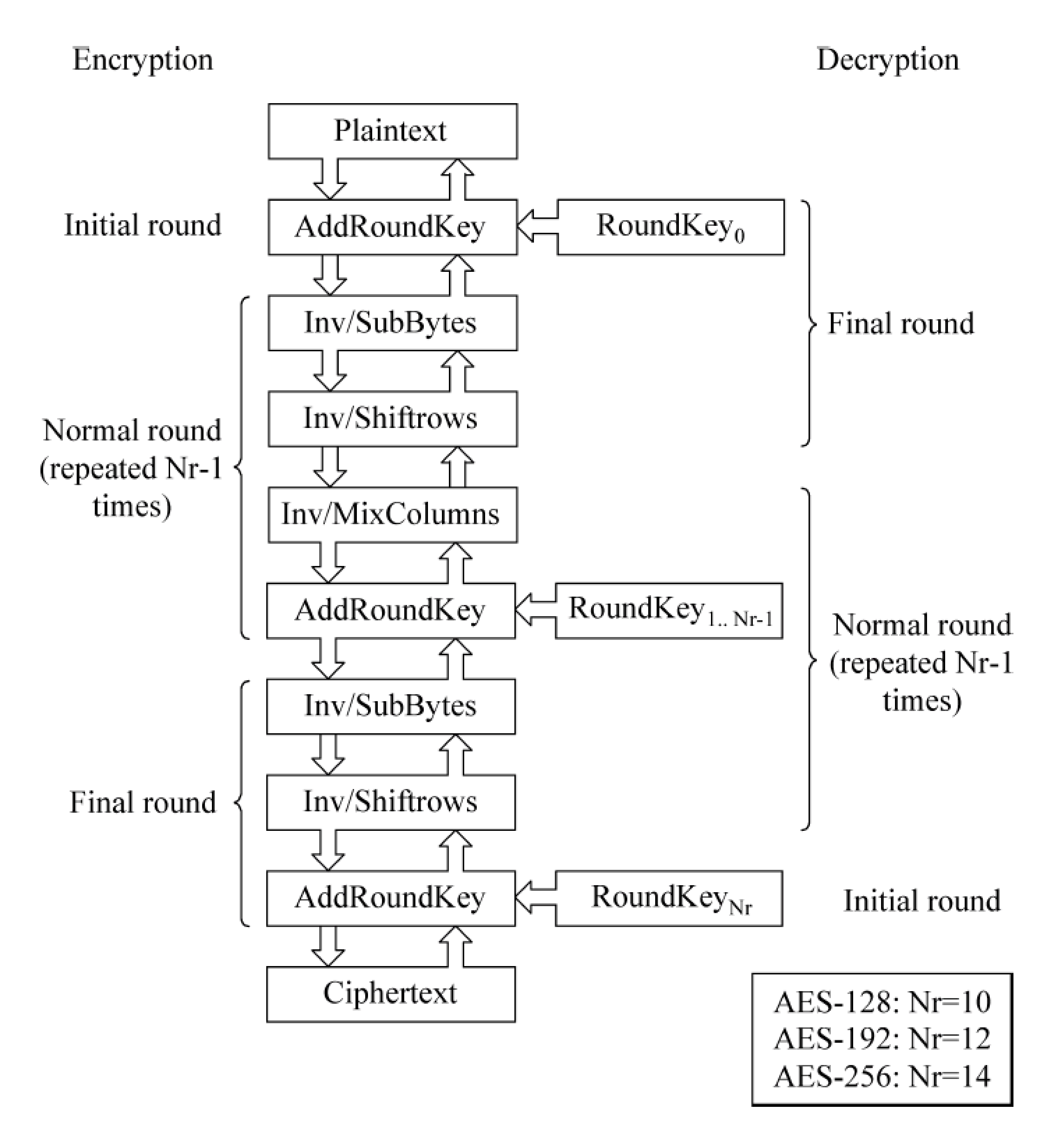


图 7.9　AES 加密算法

私有密钥 k_2 才能解密信息，一般数学表达为

$$c = E_{k_1}(m), \quad m = D_{k_2}(c), \quad m = D_{k_2}(E_{k_1}(m))$$

其中，k_1 称为公开密钥，k_2 称为私有密钥，E_{k_1} 和 D_{k_2} 可以互换使用(用于数字签名)。

1. 公钥密码思想

公钥密码的构建是通过寻找一个具有参数的困难的数学问题，利用信息的不对称，掌握主动权，设计密码。这种方法将对手破解密码的问题转换为对该数学问题的求解，如果知道参数，则求解密码很容易。因为理论证明该数学问题是困难，因此密码是经得起攻击的。比如，求离散对数问题的困难性。已知 x，计算 $y=b^x \bmod p$ 是不难的，但给定 y，求 x 是很困难的。

Diffie 和 Hellman 在“密码学新方向”这篇文章中提出了公钥密码的思想，并提出了一个 Diffie-Hellman 密钥算法，而英国的 Ellis 在 20 世纪 50 年代已经提出类似思想，但是因为保密因素，没有为人所知。

公钥是任何人都可以用来进行加密信息的，不过只有相应的私有秘钥才能解密信息，因此保证了信息只被特定的人获取。

这个公钥相当于是一个上下两口的密箱：所有人都可以通过上口送入信息；而只有极少数人拥有下口的钥匙，即密钥，进而可以提取出众人所递交的信息。通过这一方式，信息便可以有组织地收集，并且保证了仅允许指定的人能接收信息。在现实生活

中，这一公钥的加密方式便可用于政府的廉政举报和企业中的选举等活动。也类似于个人的电子邮箱，任何人都可以给邮箱所有人发信，但只有邮箱登录密钥的人才能打开邮箱并收到相应的邮件。

2. 常用公钥算法

常用公钥算法包括 RSA 算法和 ECC（椭圆曲线密码算法）

RSA 算法是由 Rivest、Shamirt 和 Adleman 于 1978 年提出，专利已到期。RSA 算法是基于 $n=p\times q$ 因子分解的困难性，其中 p、q 为超大素数（>1024b）。

ECC 由 N. Koblitz 和 A. Menezes 于 1985 年提出，没有专利。加解密密钥短，运算速度比其他公钥算法（如 RSA）快，所以受到各国安全专家和密码学家的高度重视。

RSA 算法的流程包括密钥产生、加密过程和解密过程。

（1）密钥产生。

① 取两个大素数 p 和 q

② 计算 $n=p\times q$

③ 计算欧拉函数 $\Phi(n)=(p-1)(q-1)$

④ 任取一个与 $\Phi(n)$ 互素的小整数 e，$1<e<\Phi(n)$

⑤ 寻找 $d<\Phi(n)$，使得 $de=1 \bmod \Phi(n)$

⑥ 公钥：$KU=\{e,n\}$

⑦ 私钥：$KR=\{d,\Phi(n)\}$

（2）加密过程：$c=m^e \bmod n$。

（3）解密过程：$m=c^d \bmod n$。

RSA 的公钥是通过运用两个随机生成的大质数的乘积生成的，而私钥是由这两个大质数运算产生。这样知道其中一个质数，另外一个质数将很容易得到。再加上接收者密文是很容易得到的，因此明文就被破解了。然而，对于不知道密钥的人来说，要找到这两个质数是相当困难的。这便符合了公钥密码的基本要求。

然而，在实际 RSA 算法的使用中，公钥产生过程存在一些问题。在 USENIX security symposium 2012 论文 *Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices* 中，Nadia Heninger 等收集了互联网的大量证书，这些证书都是公开的。证书中含有 RSA 加密方法的公钥，通过分析两个质数的乘积。如果两个公钥中存在共同质数，它便可以通过辗转相除法得到这个共同质数，达到破解两个证书的目的。

3. 数字信封

数字信封（Digital Envelope）就是信息发送端用接收端的公钥加密，通信密钥（即对称密钥）成一个数字信封。然后接收端用自己的私钥打开数字信封，获取该对称密钥 SK，用它来解读收到的信息。

7.3.5 密码哈希函数

1. 密码哈希函数的要求

哈希(Hash)函数也称为杂凑函数,其本质是一种压缩函数,符合安全密码学的特性,对任意长度的信息,经过哈希函数后,压缩成固定长度的信息,比如 64。哈希函数主要用于数字签名和反篡改等。

密码哈希函数必须具有以下性质。

(1) 单向性。已知 $c=\mathrm{Hash}(m)$,求 m 是困难的。

(2) 快速性。已知 m,计算 $\mathrm{Hash}(m)$是容易的。

(3) 无碰撞性。已知 $c_1=\mathrm{Hash}(m_1)$,构造 m_2,使 $\mathrm{Hash}(m_2)=c_1$ 是困难的。

(4) 敏感性。$c=\mathrm{Hash}(m)$,c 的每一位都与 m 的每一位相关,并有高度敏感性,即每改变 m 的一位,都将对 c 产生明显影响。

2. 密码哈希函数的构建

密码哈希函数在构建的过程中必须保证任何碰撞抵制的压缩函数 f 可以被扩展为 CRHF,Merkle 元方法为从 f 扩展为 CRHF 提供了有效的方案。Merkle-Damgard 增强方法——从压缩函数 f 出发,f:$\{0,1\}b+n\rightarrow\{0,1\}n$,如图 7.10 所示。之后进行反复迭代操作,如图 7.11 所示。图 7.12 给出了 Keccak 海绵构造哈希函数的方法,图 7.13 给出了根据 SipHash 原理构造哈希函数的方法。

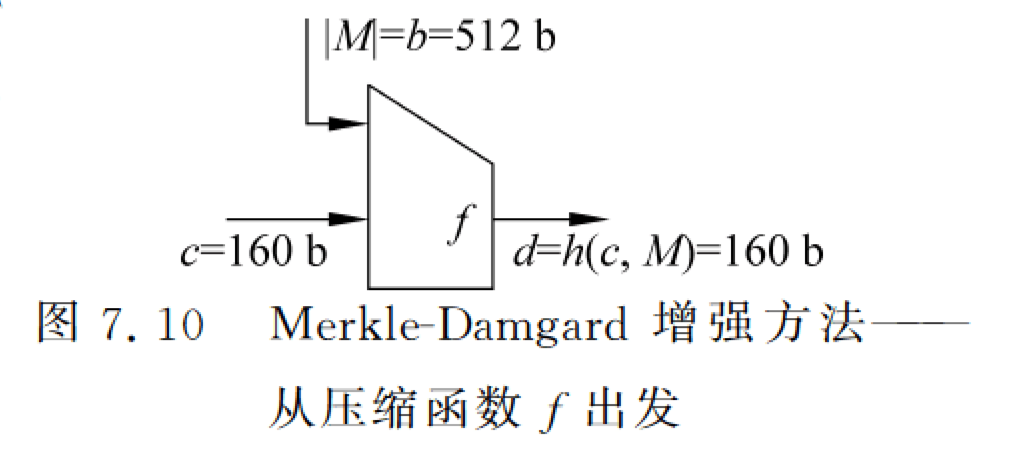


图 7.10 Merkle-Damgard 增强方法——从压缩函数 f 出发

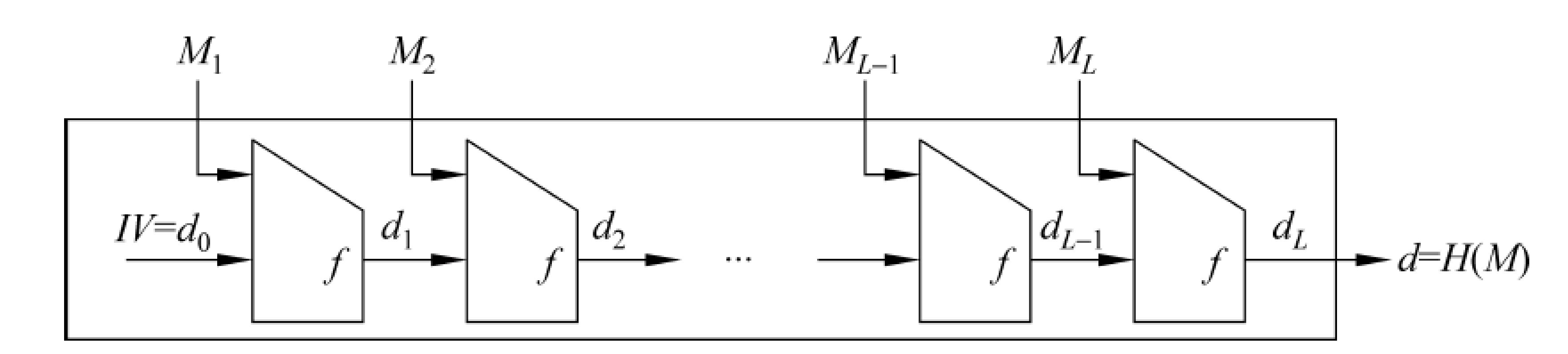


图 7.11 Merkle-Damgard 增强方法——反复迭代

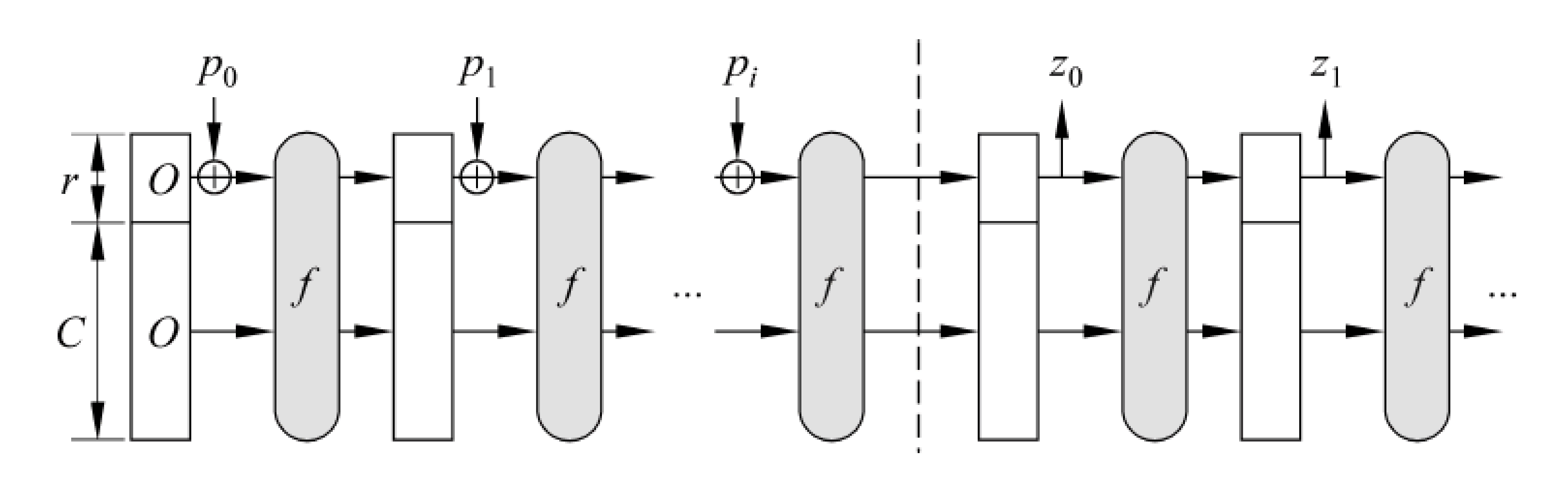


图 7.12 Keccak 海绵构造方法

哈希函数能将原有信息转换成编码,但通过编码却极难还原出原有信息。并且,原

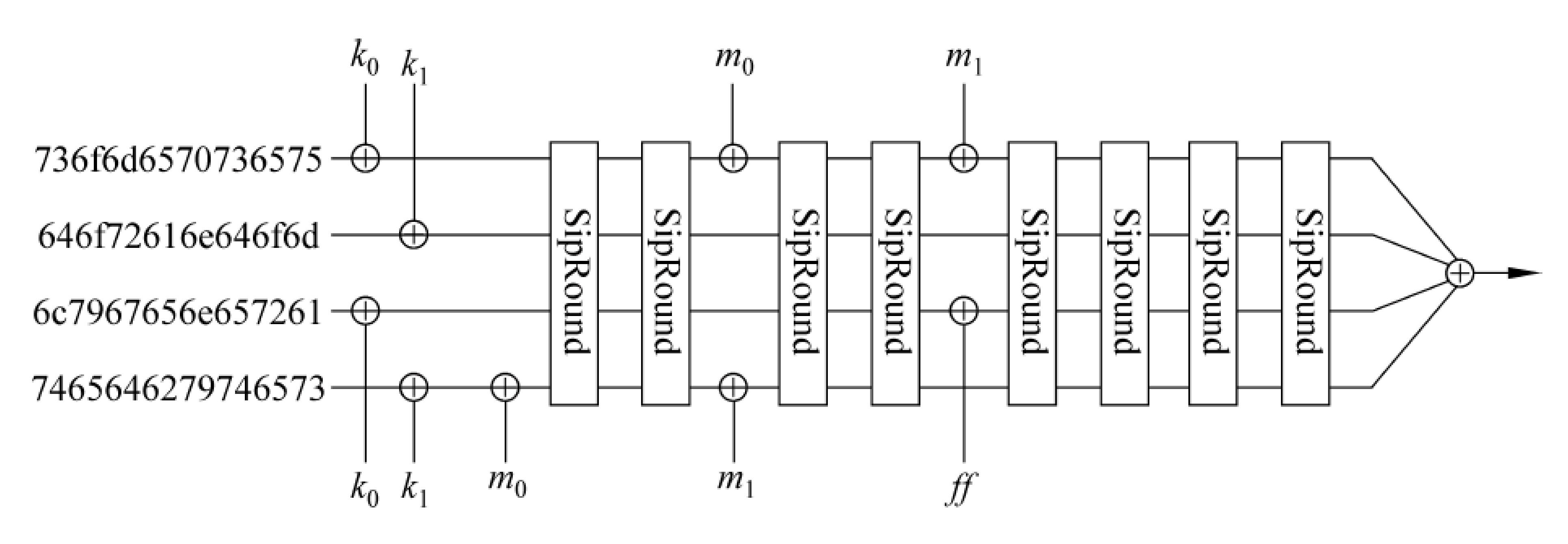


图 7.13　SipHash 原理

有信息微小的改变会使最终编码结果面目全非。它可以用作保证信息的完整性，因为无论信息脱漏还是被破坏，都会使得哈希函数输出结果变化。然而，破解哈希函数并不需要真正将它反解出来，只需要找到具有较大概率的碰撞算法就可以了。

3. 安全哈希函数(SHA)

美国国家标准技术局和国家安全局设计了与美国数字签名标准(DSS)一起使用的安全哈希算法。1995 年 4 月公布了修改版，将 SHA 称为 SHA-1。目前 SHA-1 已经被攻破，建议采用 SHA-256 和 SHA-512。

4. 数据摘要

数据摘要(Message Digest)过程如图 7.14 所示，将原文通过哈希函数运算，生成有效的密文。

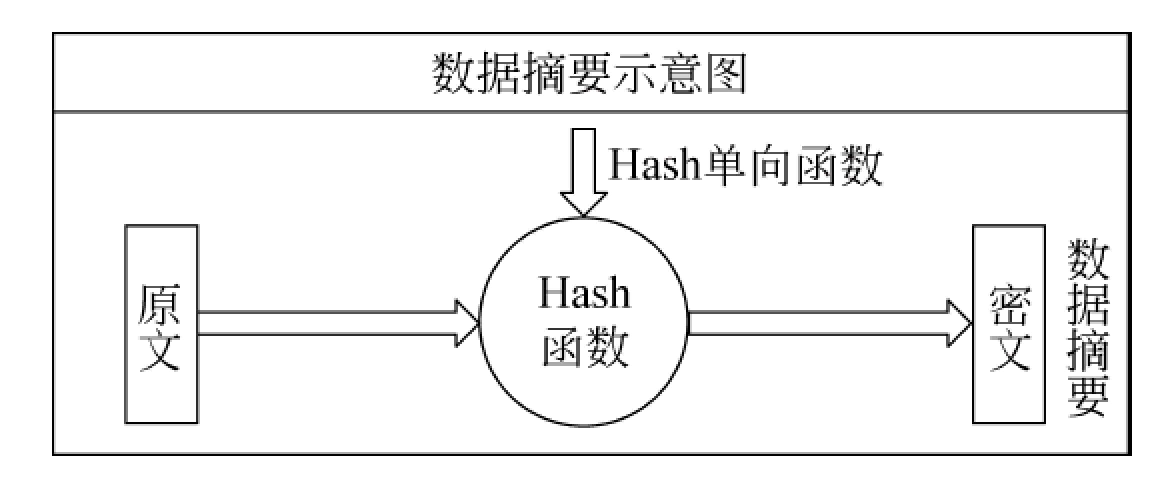


图 7.14　数据摘要示意图

7.3.6　组合应用

1. 数字签名

数字签名(Digital Signature)是指用密码算法对待发的数据进行加密处理，生成一段数据摘要信息附在原文上一起发送，接收方对其进行验证，判断原文真伪。数字签名适用于对大文件的处理，对于那些小文件的数据签名，则不预先做数据摘要，而直接将原文进行加密处理。数字签名提供数据完整性保护和提供不可否认性服务。

2. 数字签名的要求

签名者事后不能否认自己的签名;接收者能验证签名,而任何其他人不能伪造签名;当双方关于签名的真伪发生争执时,第三方能解决双方之间的争执,图 7.15 给出了一个具有数据摘要的数字签名。

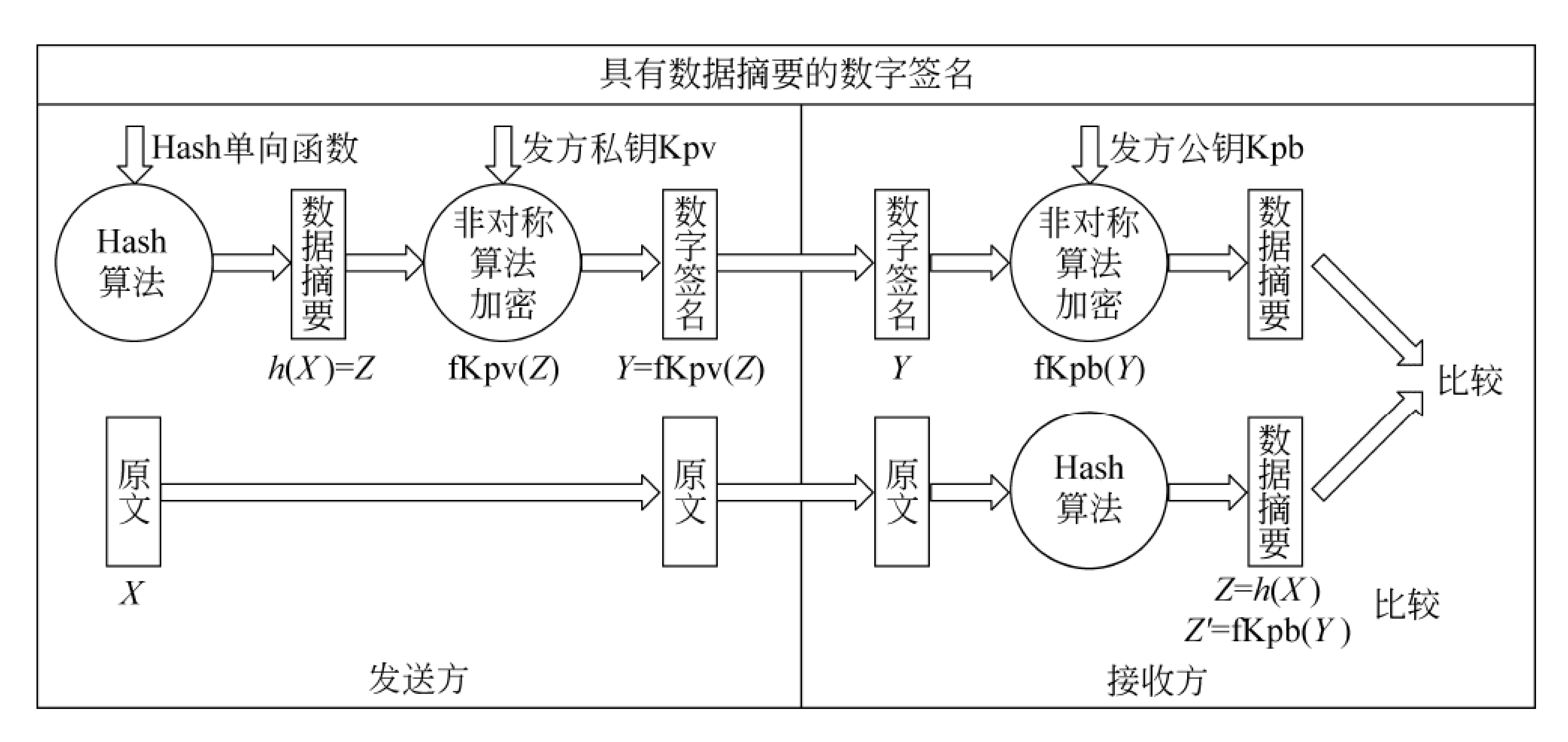


图 7.15　具有数据摘要的数字签名

3. 消息检验码

消息检验码(Message Authentication Code,MAC)也称为消息认证码,是一种需要密钥参与的哈希函数,采用这种方法也可以实现数据完整性服务。

1) HMAC 标准

HMAC 即 Hash-based Message Authentication Code。

哈希函数(如 MD5、SHA-1)能防止内容篡改、序号篡改、计时器篡改,但不能防止伪装。因此,需要对消息进行鉴别。

HMAC 被认定为 IETF RFC 2104,并被其他的 Internet 协议(如 SSL)所使用。

2) HMAC 的设计思想

(1) 无须修改即可使用现成的哈希函数。

(2) 当出现或获得更快的或更安全的哈希函数时,对算法中嵌入的哈希函数要能方便地进行替换。

(3) 保持哈希函数的原有性能,不会导致算法性能降低。

(4) 使用和处理密钥的方式很简单。

(5) 基于对嵌入哈希函数合理的假设,对鉴别机制的强度有相应密码编码分析。

4. 数字证书

数字证书(Certificate)是公钥框架 PKI 的起点,信任的载体,如图 7.16 所示,包括主体身份及公钥,认证机构及数字签名。

目前应用最广的是 X.509 证书，它符合 ISO/IEC/ITU-T X.509 标准的数字证书，参见 IETF RFC 5280。X.509 是 PKI(Public Key Infrastructure)和 PMI(Privilege Management Infrastructure)的 ITU-T 标准，与 X.500 同时发布。

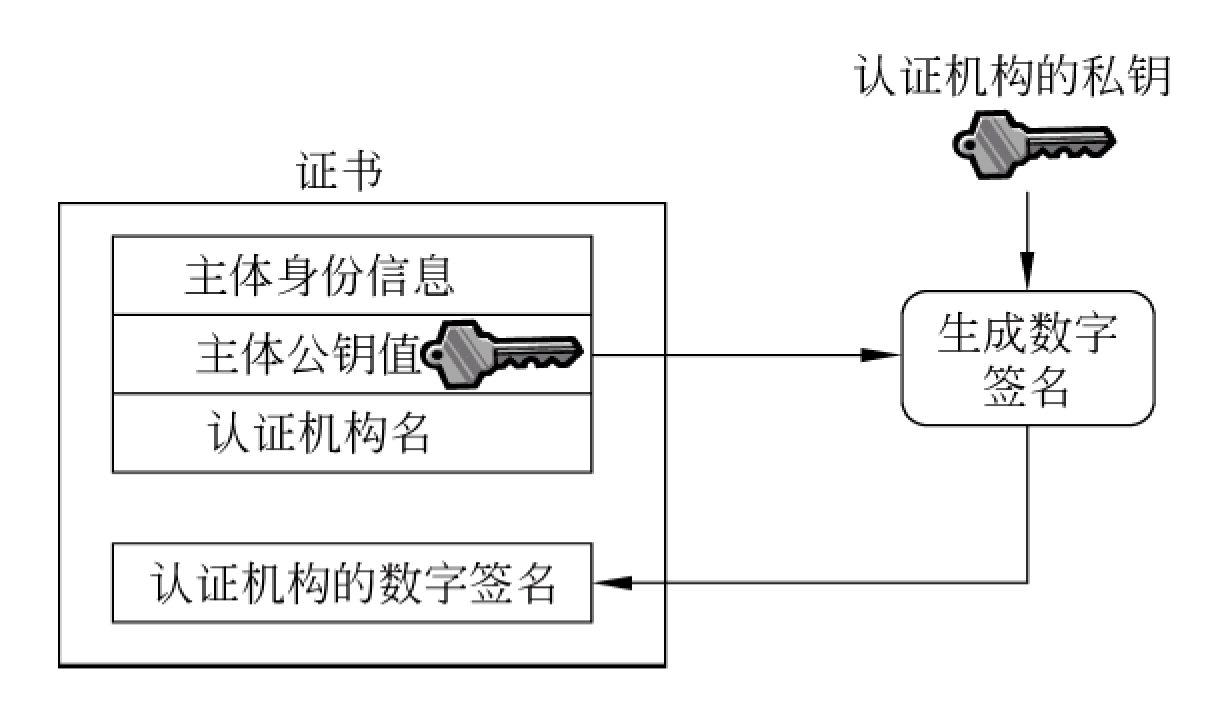


图 7.16 数字证书的制作过程

1988 年，ITU-T X.509(原 CCITT X509)作为 X.500 目录服务系统的一部分，即 X.509 version 1。1993 年 X.509 version 2 增加两个新字段，1997 年 X.509 version 3 进一步完善，增加扩展项。2001 年增加权限管理框架 PMI。2005 年增加代理服务(Delegation Service)。2009 年增加跨域授权(Interdomain Authorisation)

X.509v1 证书内容包括 OSI 参考模型的安全体系结构定义、目录模型定义和认证框架定义。X.509v3 证书参见 IETF RFC 5280，目前正在出 version 4(Draft)，即 X.509v4。X.509v4 标准中主要涉及以下几个方面：公钥数字证书认证框架、属性证书认证框架、使用证书的目录认证框架。

典型的一份 X.509 数字证书，可以由如下方法打开。打开 IE 浏览器，进行如下操作：

单击“工具”→“Internet 选项”→“内容”→“数字证书”命令。或者单击 Tools→Internet Options→Content→Certificates 命令。

7.4 互联网中的信任

信任(Trust)是整个社会正常运行的基本社会关系，按照一般定义：一个事物是可信的，意味着其身份(Identity)是可确定的，其行为(Behavior)是可预期的。

信任在电子世界网络情景下依然适用，在网络空间中信任关系的载体，信任关系的建立、确认、维护、传递和终止等过程，是通过公钥基础框架(Public Key Infrastructure，PKI)和数字证书等技术来实现的。

互联网上流行的一句话是：“在互联网上，没有人知道对方屏幕前是一只狗还是一个人”。在这种情况下，如何建立可信的网络空间？互联网机器之间的信任，是通过人为绑定在物理客观存在的一个客体上。机器之间的通信信任，是人为强加上的。但是人化的信任是不坚固的，需要建立在密码学的基础上。

类似公安局颁发公民身份证的方法，PKI 框架采用给每个信任的机器颁发数字证

书，这相当于身份证表示人的 ID，数字证书（Digital Certificate）在网络中的对应机器的 ID。

简单地说，数字证书是权威机构（CA）颁发给个体用户的、个体用户之间用来辨识身份的证明。在网络上通过交互，验证数字证书，可以在一定程度上保证交互双方的可信性。颁发数字证书的权威机构（CA）是 PKI 框架的核心，权威机构（CA）之间的一种等级结构就是 PKI 集中式信任体系模型，如图 7.17 所示。

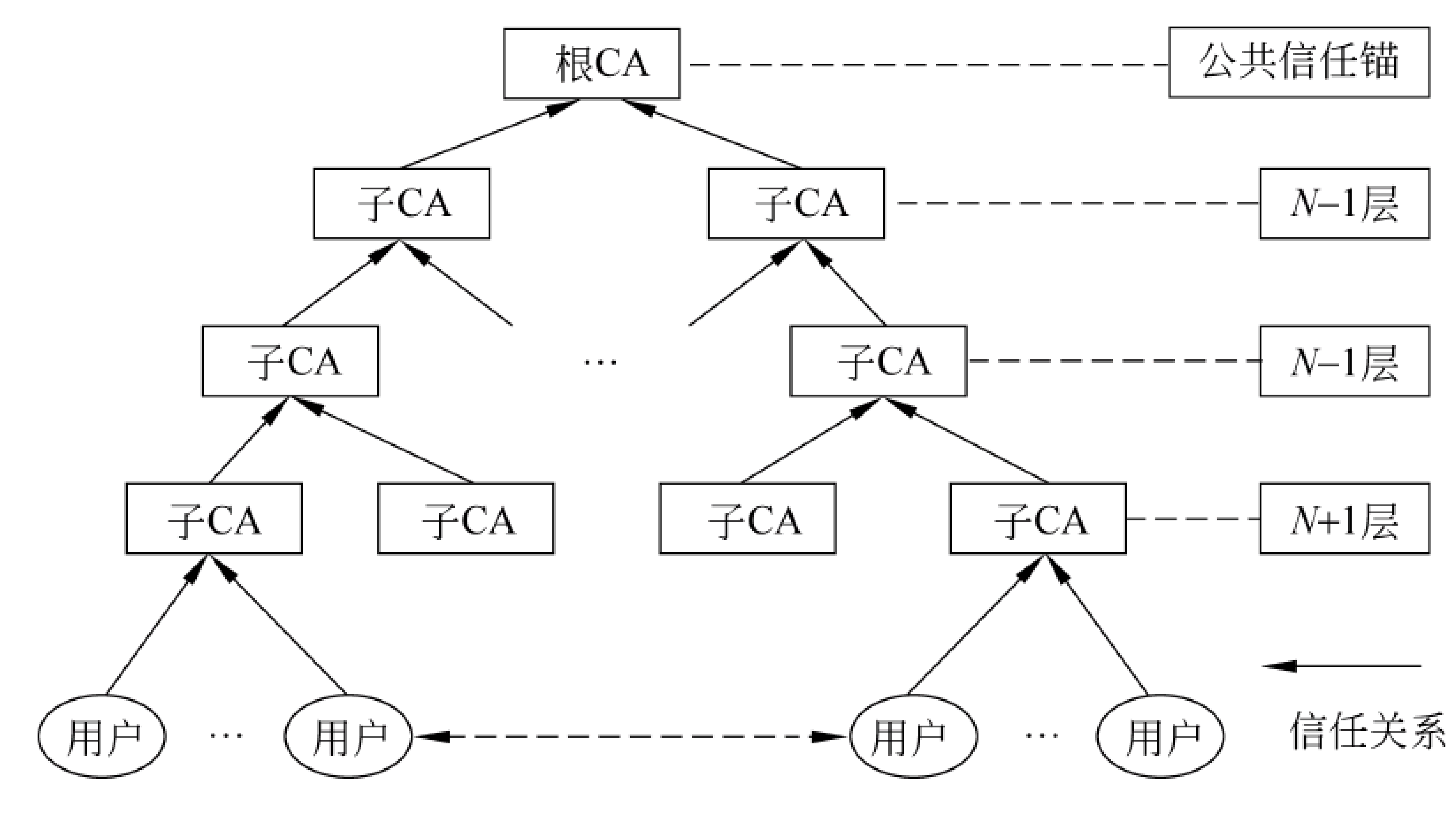


图 7.17　PKI 框架可信性认证体系

7.5　可信计算

可信计算（Trusted Computing）通过 TPM 技术，能够增强计算平台的可信性。

（1）可信计算平台 TP 采用内嵌的硬件化的密码模块确保身份与根信任。类似与手机终端的 SIM 卡，能够唯一标识每个计算平台。基于硬件密码模块的方案比软件方案更安全。

（2）可信计算平台 TP 从系统启动开始进行硬件与软件的验证。

（3）可信计算平台通过平台身份认证来向交互方证明自己的可信性。

采用 PKI 框架，采用信任状或证书来保证交互双方的身份和平台的安全性。

但是，可信计算也存在着很多问题，比如证书由谁签发，安全代价高，用户隐私泄露。

常用可信计算应用有 Microsoft 的 BitLocker 文件加密系统。目前绝大多数笔记本都安装了 TPM 或 TCM 芯片，如果要使用，只要在 BIOS 中启用 Security Chip 就可以了。

7.6　无线网络安全

随着无线局域网技术的逐步完善和普及，越来越多的个人、企业和公共场所建立了自己的无线局域网。无疑，无线局域网因其不受物理连接限制的特性极大地方便了用

户联网的需求，但与此同时，也为黑客等网络攻击者破解局域网络密码提供了可乘之机。因此 IEEE 802.3 提出了若干无线网络安全协议以试图保护无线局域网的安全，目前比较重要的协议机制包括如下 3 种：WEP、WPA 和 WPS，下面将一一展开它们的特点和安全性质，借助这些分析，我们可以发现破解 WPS 协议的可行性以及其重要安全意义。

7.6.1 WEP 技术

Wired Equivalent Privacy（WEP）协议技术，中文名为有线保密协议，是于 1999 年 9 月通过的 IEEE 802.11 标准的一部分，采用 RC4（Rivest Cipher）串流加密技术达到机密性，并使用 CRC-32 校验和保证完整性。其具体加密方法是把初始（IV）向量叠加 40 或 104 位的密钥后，经过 RC4 技术实现加密，其具体流程如图 7.18 所示，RC4 算法如图 7.19 所示。

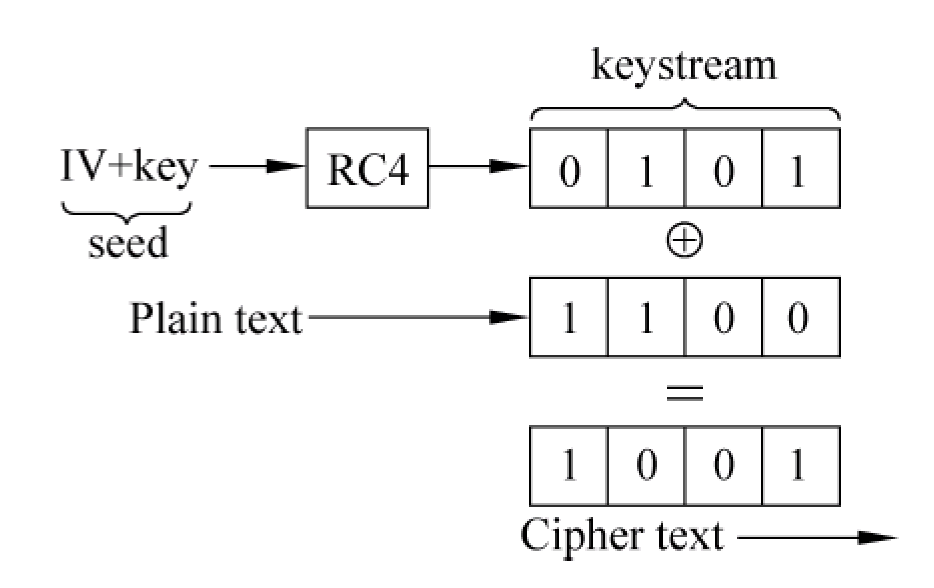


图 7.18　WEP 加密过程

WEP 技术于 2001 年被公布为不安全的网络，其主要缺陷在于使用的 40 位或 104 位的密钥必须由人工输入并且不会改变，导致通过利用 RC4 加解密和 IV 的使用方式等特性，就可以在几个小时甚至几分钟内将密码猜出。2005 年，美国联邦调查局的一组人展示了用公开可用的工具可以在三分钟内破解一个用 WEP 保护的无线局域网络。

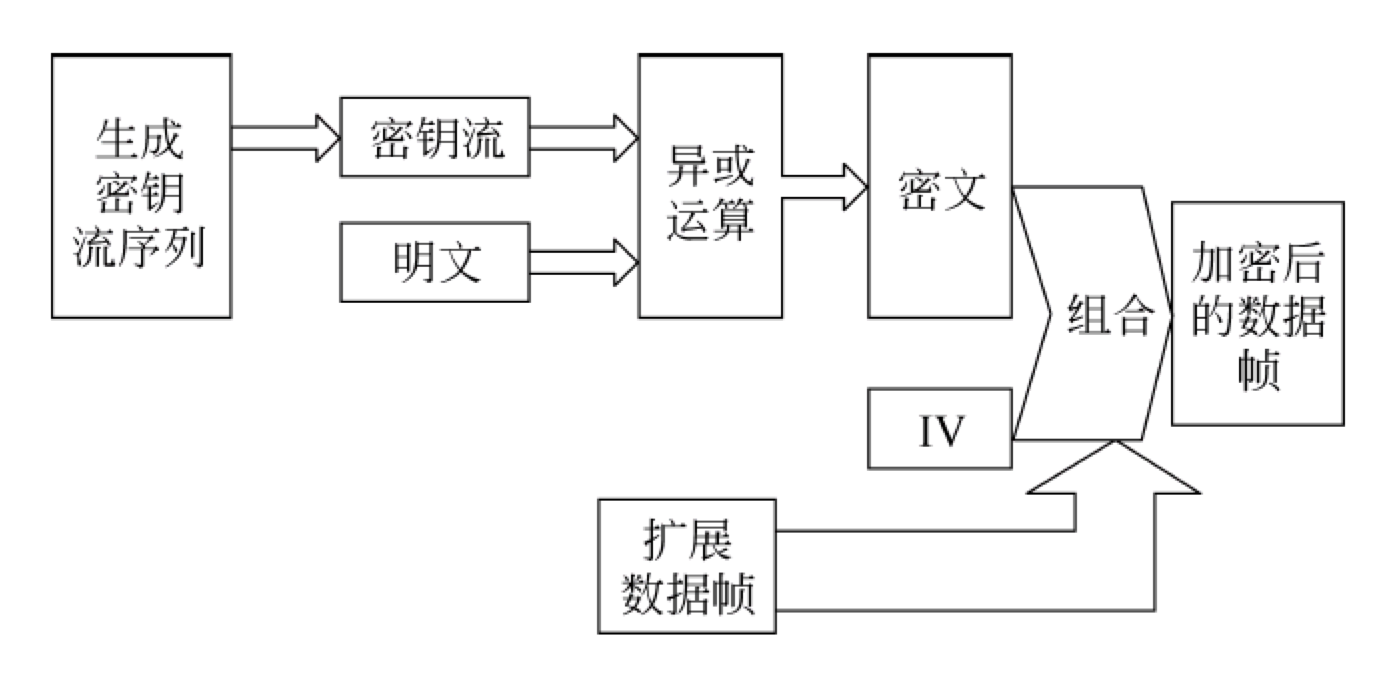


图 7.19　RC4 加密算法

由于 WEP 安全性的丧失，WEP 对于无线局域网络安全保护的意义也就不复存在。很快地，2003 年 WEP 就被新的 WPA 技术所替代，WEP 便成了无线局域网安全协议中的历史。

7.6.2 WPA/WPA2 技术

WPA/WPA2 全名为 Wi-Fi Protected Access，中文名为 Wi-Fi 网络安全存取技术，它是 IEEE 为了解决 WEP 出现的安全漏洞而提出的新的技术，在安全性能上比 WEP 协议出色很多。区别于 WEP 的静态密钥的缺陷，WPA 使用了 TKIP（Temporal Key Integrity Protocol），该协议会为每一个包动态生成一个全新的 128b 的密钥。由

于 TKIP 的动态特性，直至目前为止，大多数的破解算法也只是捕获认证包后进行字典枚举方式破解。而这种方式在面对比较复杂的密码时，其破解时间可能是以年为单位计算的，因此在一般场合中，WPA/WPA2 技术已经达到了用户所希望的安全保证。

正是由于 WPA 技术在安全性方面的卓越表现，目前绝大多数的 Wi-Fi 路由器使用的都是 WPA 加密技术，因此时至今日，WPA 保护的无线局域网络仍被人们视为一种相对安全的网络方式。

7.7 无线网络攻击示例

假如现在流行的无线路由器安全协议普遍使用 WPA/WPA2，那么破解就成了一个难度很大的目标，但是 WPA/WPA2 的一个劣势在于设置复杂。用户新建一个无线网络时，必须在接入点手动设置网络名（SSID）和安全密钥，然后在客户端验证密钥以阻止"不速之客"闯入。这整个过程需要用户具备 Wi-Fi 设备的背景知识和修改必要配置的动手能力。对于一些对无线安全与网络知识了解甚少的用户，可能宁可选择根本不加密也不去选择配置 WPA。因此，IEEE 在推出 WPA 技术的同时，还提供了一种替代配置方式，即使用 PIN 码的 WPS 技术。

7.7.1 WPS 安全

无线网保护设置（Wi-Fi Protected Setup，WPS）非常重要。为了简化无线局域网的配置工作，WPS 帮助用户自动设置网络名（SSID）、配置 WPA 数据编码及认证功能，用户只需输入个人信息码（PIN）或按下按钮（按钮设置，或称 PBC），即能安全地接入无线网络。从网络安全的角度讲，WPS 可以说是与 WPA 相平行的一种验证方式，只要客户端输入了正确的 PIN 码或按钮设置，路由器就会向客户端自动发送 WPA2 的密码文本，使客户端进入网络。

WPS 技术是 Wi-Fi 标准化组织为了面向普通用户简化路由器安全设置而设计的。所有采用 WPS 的路由器都提供以下 3 种"傻瓜式"的方式让普通用户从客户端连接到加密的路由器。

（1）用户的计算机尝试请求用 WPS 连接路由器，接着用户在路由器上单击一个按钮，请求验证通过。

（2）用户的计算机尝试请求用 WPS 连接路由器，接着用户在路由器的管理界面上输入 PIN 码，请求验证通过。

（3）用户在计算机用 PIN 码连接路由器，请求验证通过。

通过以上任意一种方法，请求验证通过后，无线路由器把配置信息（包括 WPA2 PSK 密码）发给客户端，然后客户端就能接入网络。

可以看到，以上第 3 种方法有一个设计上的缺陷，即不需要用户在物理上接触路由器就能连接路由器，相当于提供了与 WPA2 平行的认证方式。而 PIN 码只是一个 8 位数（共 10^8 种可能），规模相比于直接暴力破解 WPA 密码是非常小的。再者，PIN 码

最后一位数字是校验位，这样破解尝试数量只剩下 10^7。下面介绍如何破解 WPS。

7.7.2 WPS 破解

无线网卡可以工作在多种模式之下。常见的有 master、managed、Ad-hoc、monitor 等模式。对于 master 模式，它主要使用于无线接入点 AP 提供无线接入服务以及路由功能。对于一般的无线网卡来说，最常见的模式还是 managed、Ad-hoc 和 monitor。managed 模式用于和无线 AP 进行接入连接。对于需要两台主机进行直连的情况下可以使用 Ad-hoc 模式，这样主机之间是采用对等网络的方式进行连接。monitor 模式主要用于监控无线网络内部的流量，用于检查网络和排错。

无线局域网的信号传输完全是以无线电波的方式进行广播传输的，这也就意味着每个人都可以用一定的装置来对无线电信号进行接收。设有无线网卡为监听模式(Monitor Mode)，网卡可以接收到所有它能够接收的无线电信号并试图进行解析，而不仅仅局限于它已连接的无线局域网。这样的模式对于无线局域网的发现机制来说有着根本的作用，也无形地提供了破解无线局域网的工具。

将网卡设置成监听模式，由于工作在监听模式下，采用了 libpcap 库便于进行底层网络操作，对于无线 AP 的 802.11 认证(Authentication)和关联(Association)操作进行处理。值得注意的是，即使完成了 802.11 关联，监听模式下的网卡仍然能收到其他网络设备的数据，需要根据 802.11 帧头的源地址和目的地址进行过滤。完成 802.11 连接后，接着进行 EAP 会话的创建(EAP Initiation)，EAP 是 WPA 和 WPA2 进行验证采用的协议。之后就进入了的 WPS 协议过程。

枚举 PIN 时，先尝试部分路由器使用的默认 PIN，如果失败则从 00000000 开始枚举。在每次枚举过程中，先对 PIN 前半部分枚举，PIN 后半部分固定不变，待 PIN 前半部分破解成功后再枚举后半部分。注意，在枚举前半部分时，后半部分最后一位是校验位，因此也需要改变。对于每一次对路由器的破解，能够破解出这个路由器的完整 PIN，密钥 PSK，破解进行得比较彻底。

WPS 的认证协议中，Enrollee 为无线路由器，Registrar 为接入者，即攻击者。无线路由器和接入设备之间互相交换了 8 条消息($M_1 \sim M_8$)，详见下面

Enrollee→Registrar: M_1 = Version||N1||Description||PK_E

Enrollee←Registrar: M_2 = Version||N1||N2||Description||PK_R [||ConfigData]||$HMAC_{AuthKey}$ (M_1 ||M_2^*)

Enrollee→Registrar: M_3 = Version||N2 ||E-Hash1||E-Hash2||$HMAC_{AuthKey}$ (M_2 ||M_3^*)

Enrollee←Registrar: M_4 = Version||N1||R-Hash1||R-Hash2||$ENC_{KeyWrapKey}$ (R-S1) ||$HMAC_{AuthKey}$ (M_3 ||M_4^*)

Enrollee→Registrar: M_5 = Version||N2||$ENC_{KeyWrapKey}$ (E-S1) ||$HMAC_{AuthKey}$ (M_4 ||M_5^*)

Enrollee←Registrar: M_6 = Version||N1||$ENC_{KeyWrapKey}$ (R-S2) ||$HMAC_{AuthKey}$ (M_5 ||M_6^*)

Enrollee→Registrar: M_7 = Version||N2||$ENC_{KeyWrapKey}$ (E-S2 [||ConfigData]) ||$HMAC_{AuthKey}$ (M_6 ||M_7^*)

Enrollee←Registrar: M_8 = Version||N1|| [$ENC_{KeyWrapKey}$ (ConfigData)] ||$HMAC_{AuthKey}$ (M_7 ||M_8^*)

E-Hash1 从 PIN 的前半部分计算得到，为了说明计算过程，引入变量 PSK1＝first 128 bits of HMACAuthKey(first half of PIN)，类似地 PSK2＝first 128 bits of

HMACAuthKey(Second half of PIN)。

无线路由产生两个 128 位的随机数(E-S1 和 E-S2),然后计算 E-Hash1 和 E-Hash2:

```
E-Hash1= HMACAuthKey(E-S1||PSK1||PKE||PKR)
E-Hash2= HMACAuthKey(E-S2||PSK2||PKE||PKR)
```

同样地,攻击者也产生两个随机数(R-S1 和 R-S2)并计算 R-Hash1 和 R-Hash2:

```
R-Hash1= HMACAuthKey(R-S1||PSK1||PKE||PKR)
R-Hash2= HMACAuthKey(R-S2||PSK2||PKE||PKR)
```

回顾 WSP 协议的消息 $M_3 \sim M_7$ 部分:

$$\text{Enrollee} \rightarrow \text{Registrar:}\quad M_3 = \text{Version}||\text{N2}||\text{E-Hash1}||\text{E-Hash2}||\text{HMAC}_{\text{AuthKey}}(M_2||-M_3^*)$$
$$\text{Enrollee} \leftarrow \text{Registrar:}\quad M_4 = \text{Version}||\text{N1}||\text{R-Hash1}||-\text{R-Hash2}||\text{ENC}_{\text{KeyWrapKey}}(\text{R-S1})||\text{HMAC}_{\text{AuthKey}}(M_3||M_4^*)$$
$$\text{Enrollee} \rightarrow \text{Registrar:}\quad M_5 = \text{Version}||\text{N2}||\text{ENC}_{\text{KeyWrapKey}}(\text{E-S1})||\text{HMAC}_{\text{AuthKey}}(M_4||M_5^*)$$
$$\text{Enrollee} \leftarrow \text{Registrar:}\quad M_6 = \text{Version}||\text{N1}||\text{ENC}_{\text{KeyWrapKey}}(\text{R-S2})||\text{HMAC}_{\text{AuthKey}}(M_5||M_6^*)$$
$$\text{Enrollee} \rightarrow \text{Registrar:}\quad M_7 = \text{Version}||\text{N2}||\text{ENC}_{\text{KeyWrapKey}}(\text{E-S2}\ [||\text{ConfigData}])||\text{HMAC}_{\text{AuthKey}}(M_6||M_7^*)$$

WPS 的安全问题在于接入者返回无线路由器试图验证 PIN 的确认消息。如果 WPS 认证失败,无线路由器 AP 会发送回一个 EAP-NACK 消息。通过该消息,攻击者可以得知 PIN 的部分正确性。这种形式的认证使得寻找正确的 PIN 的尝试次数大大降低。

另外,WPS 标准把 PIN 分成两段,分别发给路由器验证(M_4 和 M_6)。在 M_4 时,路由器知晓了 R-S1,则可以验证 PIN 的前半部分。在 M_6 时,路由器知道了 R-S2,则验证后半部分。任何一个阶段验证失败,则接收方返回 EAP-NACK 信息。由于两部分的验证时相互独立的,这样可以分两部分穷举 PIN,也就是 10000+1000=11000 次。

不修改 WPS 的设置,唯一防范攻击的方法是打开 MAC 地址过滤来阻止不受欢迎的接入设备。然而,通过检测和路由器有现成连接的设备的 MAC 地址,攻击者可将其设置为自身 MAC 地址,伪装成该设备,从而可以很轻易地绕过 MAC 地址过滤。

7.8 安全 HTTP 连接

7.8.1 SSL/TLS 的工作原理

SSL/TLS 协议不是简单的单个协议,而是一个两层协议,它包含的协议规范有 SSL/TLS 握手协议、SSL/TLS 修改密码规范协议、SSL/TLS 报警协议、SSL/TLS 记录协议。SSL/TLS 握手协议用于协商加密算法、交换密钥等;SSL/TLS 修改密码规范协议用于更新 SSL/TLS 连接使用的密码组,协议由一个仅包含一字节值为 1 的消息组成,用于通知对方改变连接状态;SSL/TLS 报警协议用于向对方传递与 SSL/TLS 相关的报警,它的消息由两字节组成,其中一个字节表示报警的级别,另一个字节表示

报警的内容;SSL/TLS 记录协议对上层数据进行压缩、加密等操作后交给 TCP 进行传输。它们的层次关系如图 7.20 所示。

SSL/TSL握手协议	SSL/TLS修改密码规范协议	SSL/TLS警报协议	HTTP
SSL/TLS记录协议			
TCP			
IP			

图 7.20　SSL/TLS 协议栈

从图 7.20 可以看出,SSL/TLS 握手协议、SSL/TLS 修改密码规范协议、SSL/TLS 报警协议在 SSL/TLS 记录协议之上,它们与 HTTP 的层级相同,HTTP 的消息可由 SSL/TLS 记录协议处理后交给 TCP。SSL/TLS 握手协议的消息可以直接由 TCP 进行传输,因为在 SSL/TLS 握手协议完成之前,SSL/TLS 记录协议还未协商采取什么样的措施对上层数据进行处理。下面将重点介绍 SSL/TLS 握手协议和 SSL/TLS 记录协议。

7.8.2　SSL/TLS 握手协议

SSL/TLS 是一个协商协议,即加密用的密钥是由通信的双方共同协商确定的,而不是事先定义好的。握手协议在数据传输之前进行,由客户端和服务器之间交互的一系列消息组成,消息是一个简单的三元组格式:(类型,长度,内容)。握手协议完成后,表明双方已经为安全通信做好了准备,包括客户端和服务器之间的相互认证、协商加密消息所用的会话密钥、生成消息认证码(Message Authentication Code,MAC)的算法。SSL/TLS 握手协议的整个过程如图 7.21 所示,由 4 个阶段组成。

阶段 1:建立安全能力。

客户端发送 client_hello 消息发起建立连接的请求,服务器端发送 server_hello 消息进行回应。这两种消息都包含如下参数:版本号、随机数、会话标识、密码组、压缩方法。其中版本用于协商使用何种版本的 SSL/TLS;随机数用于在密钥交换时防止重放攻击;会话标识用于协商是否重用或者新建一个连接;密码组按优先级列出了各自支持的密码算法,用于协商加密算法或 MAC 算法等;压缩方法协商传输前采用何种方法对数据进行压缩。

阶段 2:服务器认证和密钥交换。

如果需要对服务器进行认证(除非采用匿名 Diffie-Hellman 方法,否则,其他密钥交换方法均需要证书消息),则服务器发送 certificate 消息将一个或一组 X.509 证书发送给客户端;如果需要,服务器发送 server_key_exchange 消息交换密钥;如果服务器不采用匿名 Diffie-Hellman 方法,则会发送 certificate_request 消息向客户端请求证书;当以上过程完成后,服务器发送 server_hello_done 消息表明 hello 和相关消息发送结束,并且将等待客户端应答。

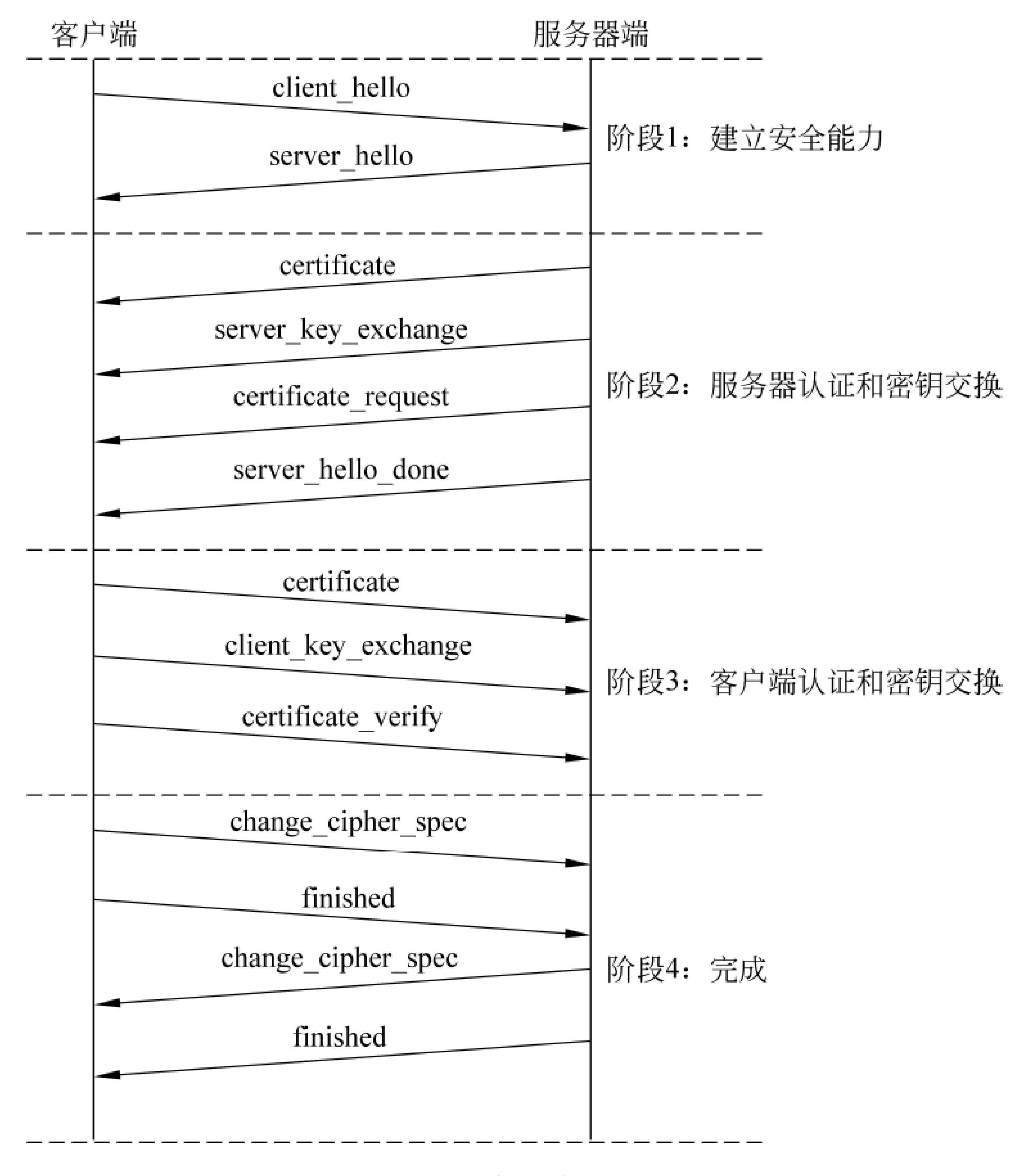


图 7.21　SSL/TLS 握手协议消息交换过程

阶段 3：客户端认证和密钥交换。

在接收到服务器的上述消息之后，客户端会对服务器的证书进行验证。如果服务器发送了 certificate_request 消息，客户端会通过 certificate 消息发送证书；之后，客户端会发送 client_key_exchange 消息进行密钥交换；在此阶段的最后，客户端还可以发送 certificate_verify 消息提供对客户端证书的精确认证，该消息是一个对客户端证书的签名消息。

阶段 4：完成。

客户端和服务器端都会发送 change_cipher_spec 消息和 finished 消息，但是需要注意的是，change_cipher_spec 消息不是握手协议的一部分，而是使用修改密码规范协议发送的，用在这里只是为了帮助说明整个安全连接建立的过程。发送 change_cipher_spec 消息是为了让对方把会话的挂起状态复制到当前状态。finished 消息是在新的算法、密钥、密码下发送的，用于验证密钥交换和认证过程的正确性。本阶段完成后，整个握手过程也完成，客户端和服务器即可开始交换应用层的数据。

从以上 4 个阶段可以看出，阶段 1 用于协商建立安全连接的参数，阶段 2 和阶段 3 进行认证及密钥交换，阶段 4 验证认证过程和密钥交换是否成功。

7.8.3 SSL/TLS 记录协议

SSL/TLS 记录协议指明了在传输应用消息之前将对消息进行何种操作和格式处理。图 7.22(a)说明 SSL/TLS 记录协议的整个操作过程。来自应用层的数据首先会被分段，然后进行压缩(也可以选择不压缩，主要取决于握手协议协商的结果)，其次加上 MAC 并加密，最后加上 SSL/TLS 记录头。经过 SSL/TLS 记录协议处理后的最终数据单元会被放入一个 TCP 段中，然后经过网络传输到达接收方，接收的收据经过解密、验证、解压、重组的逆向操作后传递给应用层的用户，至此，一个完整的传输过程完成。

应用层的数据经过 SSL/TLS 记录协议处理后格式如图 7.22(b)所示，处理后的数据可分为两个部分：SSL/TLS 头和加密部分。SSL/TLS 记录头由内容类型、主版本号、从版本号、压缩长度 4 个字段组成。

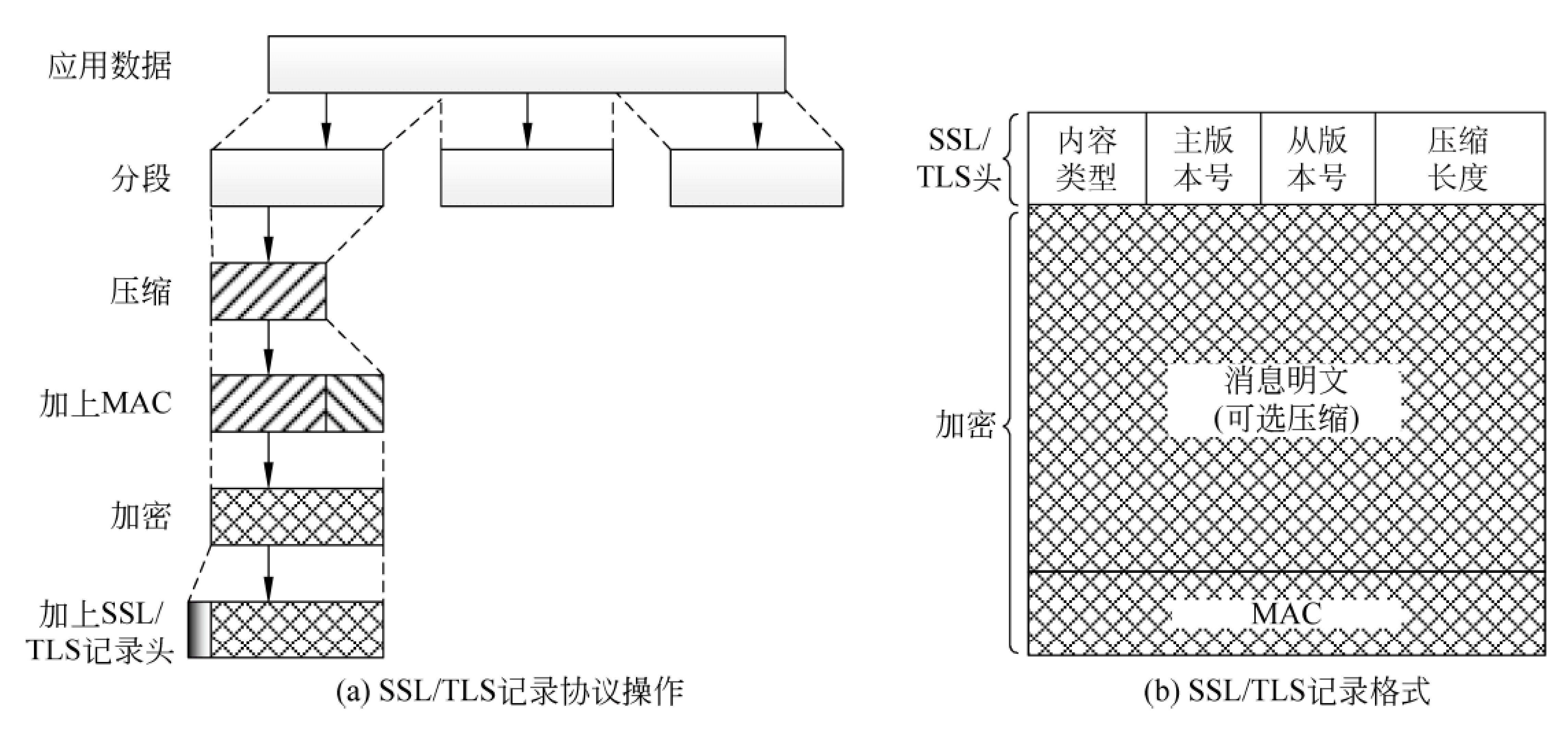


图 7.22　SSL/TLS 记录操作和格式

7.9　安全 HTTP 连接攻击示例

7.9.1 针对 SSL/TLS 的攻击

针对 SSL/TLS 的攻击非常多，这些攻击要么欺骗客户端去获取用户的敏感信息，要么欺骗服务器去进行非法的访问，但是在这里我们不是简单地将 SSL/TLS 攻击分为针对客户端的攻击和针对服务器的攻击，而是将 SSL/TLS 的攻击分为三类：与机制有关的攻击、与实现有关的攻击、与信任模型有关的攻击。

SSL/TLS 协议与其他的互联网协议一样，也是由一组规范和机制组成，再完美的机制也可能存在薄弱环节，无可避免地给攻击者留下可乘之机。从 SSL/TLS 的设计机制上找漏洞，进而进行攻击的这一类行为称为与机制有关的攻击。

尽管 SSL/TLS 的某些设计机制可能不存在缺陷，但是在实际实现中，由于某些策

略暂时无法实现，进而采取了折中的策略，攻击者就有可能从具体的实现上找漏洞进行攻击，这类攻击称为与实现有关的攻击。

SSL/TLS 协议是建立在信任模型（即依靠第三方机构给客户端或服务器签发证书）的基础之上的，因此，如果信任模型存在问题，整个 SSL/TLS 的安全性也就无从谈起。很多攻击者意识到从 SSL/TLS 的机制上进行攻击存在一定的难度，如果把目光转向信任模型可能会达到事半功倍的效果，攻击者进行了诸如伪造证书等攻击，这类攻击被称为与信任模型有关的攻击。

7.9.2 与机制有关的攻击

1. SSLstripping Attack

在 2009 年的黑帽（Blackhat）会议上，公开了一种新的针对 SSL/TLS 的攻击，它就是 SSLstripping Attack。简言之，SSLstripping Attack 将 HTTPS 协议的安全 S 剥除（strip）掉，使用户的敏感信息通过 HTTP 传输，最终达到窃取用户敏感信息的目的。

图 7.23 通过对比的方式展示了 SSLstripping 攻击的过程。在正常模式下（见图 7.23(a)），用户访问某个站点，例如 http://www.example.com，如果需要登录等操作，服务器会返回一个通过 HTTPS 协议加密过的页面，例如，https://login.example.com，接下来用户会填写用户名和密码等，由于整个消息是通过 HTTPS 协议传输的，所以用户的敏感信息会得到保护。而在 SSLstripping Attack 模式下（见图 7.23(b)），用户与服务器之间的交互信息都会被攻击者截断，攻击者会将用户的请求发送给服务器，一旦服务器返回以 HTTPS 协议加密的页面时，攻击者就会将该页面劫持，然后通过 HTTPS 协议给用户发送一个相同或相似的页面，接下来的情形可想而知，当用户在 HTTPS 页面上填写信息时，这些信息都完全暴露给了攻击者。



图 7.23 用户在正常模式下和在 SSLstripping Attack 模式下与服务器的交互过程

通过以上过程可以看出，SSLstripping Attack 是中间人攻击（Man In The Middle，MITM）的一种模式，它在技术上并没有很高的要求，而是通过用户的访问习惯等将用户引入了攻击页面。如果用户在访问敏感页面时都会手动输入以 HTTPS 开头的地

址，那么这种攻击就不会得逞；相反，如果用户通过导航等链接访问敏感页面时，往往会被引入攻击的陷阱。Chrome 浏览器在高级设置中可强制使用 HTTPS 访问任何网站，从而部分解决该问题。

2. Cross-Protocol Attack

在 ACM CCS 2012 上，N. Mavrogiannopoulos、F. Vercauteren、V. Velichkov 等描述了一种适用于所有 TLS 版本的 Cross-Protocol 攻击，它可视为针对 SSLv3 的 Wagner and Schneier Attack 的扩展。从 SSL/TLS 的工作原理可以看出，客户端和服务器可能支持不同种类的密钥交换算法，Cross-Protocol Attack 通过对密钥交换参数进行错误的解释来达到攻击的目的。一种典型的情形是，如果服务器支持 ECDH（Elliptic Curves Diffie-Hellman）密钥交换算法，客户端支持 DH（Diffie-Hellman）密钥交换算法，攻击者会模仿服务器的行为，将 ECDH 参数解释为普通的 DH 参数，从而取得客户端的信任。但是这种情形对开源的服务器并不适用，因为它们不支持 ECDH 密钥交换算法。从以上分析可以看出，Cross-Protocol 攻击通过模仿服务器的特征来取得客户端的信任，进而以服务器的身份与客户端通信来到达窃取信息的目的。

3. Renegotiation Attack

在 SSL/TLS 协议中，通信双方在已建立安全连接的情况下，可以重新协商密钥参数，然后使用新的密钥来加密消息进行通信，密钥协商过程必须在之前建立的安全通道中进行，但是这样并不能保证整个重协商过程不会被攻击者利用。E. Rescorla 提出的重协商攻击（Renegotiation Attack）就是利用重协商的漏洞来模仿客户端的特征，然后去欺骗服务器的一种攻击行为。

Renegotiation Attack 的原理如图 7.24 所示。攻击者首先会通过 SSL/TLS 握手协议向服务器发起建立 SSL/TLS 安全连接的请求，在安全通道建立之后，攻击者可以与服务器之间进行一些常规的通信。当攻击者嗅探到客户端将要向服务器发起建立安全连接的请求时，它会劫持客户端发送的握手包，然后通过自己先前建立的安全通道发送给服务器。由于握手包是通过攻击者的安全通道发送的，服务器在接收到握手包后，就会误认为这个握手包是由攻击者发送的，即认为攻击者发起了一个重协商的请求。由于握手包本来来自客户端，这样一来，服务器就会误认为攻击者具有客户端的某些权限，接下来，客户端发往服务器的流量就会被攻击者插入具有某种企图的流量，而服务器又盲目的相信这些流量都是合法的请求，结果就会造成严重的后果。

7.9.3 与实现有关的攻击

1. 伪随机数 PRNG Attack

SSL/TLS 协议的设计多处是使用了随机数，但在实际实现中尚不能得到真正意义

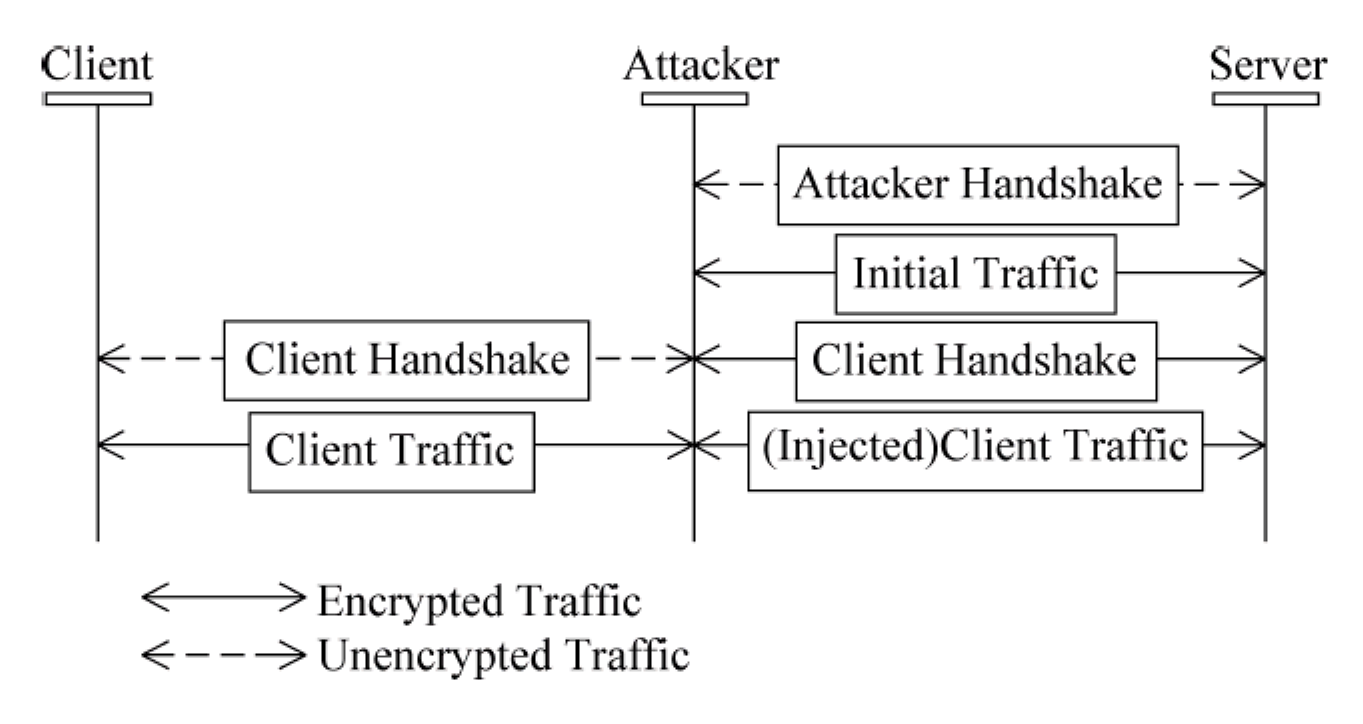


图 7.24 Renegotiation Attack 原理

上的随机数，目前通常采用伪随机数发生器(Pseudo Random Number Generator，PRNG)生成近似随机的数。伪随机数由于缺乏随机数不可预测性的特点，常常成为攻击的目标。人们把利用一定的手段对 PRNG 生成的随机数进行预测的行为称为 PRNG 攻击。早期版本(低于 1.22)的 Netscape 浏览器使用的 PRNG 就经常成为攻击的目标，攻击者可以成功预测 SSL/TLS 的会话密钥。

2. OpenSSL 的心脏出血攻击

OpenSSL 是目前互联网上使用的最广泛的开源的 SSL/TLS 软件。披露于 2014 年 4 月的 OpenSSL Heartbleed 攻击一时间引起网络安全界的轰动。OpenSSL Heartbleed Attack 充分利用了 OpenSSL 的一个扩展功能——OpenSSL Heartbeat Extension 的一个漏洞。Heartbeat Extension 作为 SSL/TLS 的一个扩展功能，已被写入 RFC 6520。Heartbeat Extension 用于测试当前的 SSL/TLS 是否处于活跃状态，避免了使用重协商的机制。

Heartbeat Extension 的原理非常简单，通信的某一方发送一个 Hearbeat Request 消息，消息由负载和负载长度两部分组成，负载通常是一个文本字符串，负载长度作为附加字段对整个负载的长度进行说明；接收方收到 Heartbeat Request 消息后，原则上应该将该消息的负载原封不动地返回给发送方，但是接收方在返回负载时不是根据负载的实际大小返回内存中的内容，而是根据消息中负载长度字段指明的大小返回内存中的内容。Heartbleed Attack 巧妙地利用了 Heartbeat Extension 的一个漏洞，如果发送方在发送 Heartbeat Request 消息时，设定一个与负载实际长度不相符的负载长度字段，比如远远大于负载的实际长度，那么接收方再根据负载长度字段的值返回内容时，就会将内存中的额外内容返回给发送方，而额外内容中可能包含用户名、密码等敏感信息，从而造成用户敏感信息泄露。

第8章 未来网络

当前互联网的使用疆域拓展到了前所未有的广阔，如工业控制网、物联网、车联网以及星际间联网。而且，这个边界还在不断地随着人类的认识和足迹而延伸。

随着更广阔的联网需求的出现，互联网协议并不一定能像先前那样可以不断地推广到新的联网领域。这些联网的问题，需要互联网的协议及技术的进一步发展和创新，以容纳越来越多的联网设备。

然而，互联网协议提出至今，40 余年没有经过大的调整。经过了这 40 余年的发展，逐渐暴露出越来越多的问题，比如安全、可扩展性、移动、应用僵化和可管理性等问题。

为了解决当今互联网存在的诸多问题，国际上许多研究机构都在探索未来互联网的设计问题，比如美国 NSF 在 2010 年资助了 4 个未来网络的研究项目，资助时间为 3 年。2013 年又增加了两个项目。这 6 个项目都宣称能解决当前互联网的主要问题，但其侧重点各不相同。

8.1 未来网络架构

8.1.1 命名数据网络

命名数据网络(NDN)项目的主要思想来源于对当今互联网上应用需求和背景改变的观察。互联网在设计之初，主要的应用需求是计算资源共享，而经过 50 多年的发展，互联网的使用已发生了巨大的变化，现在互联网的主要使用需求是内容的获取和分发。虽然应用发生了变化，但互联网的体系结构仍然是主机对主机(host-to-host)通信模式，对于以发布和获取信息为主的互联网，通信模式存在明显的不足，比如每次存取内容，都要间接映射到内容所在的设备。为了解决这个问题，NDN 采用名字路由，通过路由器来缓存内容，从而使数据传输更快，并能提高内容的检索效率。NDN 的具体实现例子，是由施乐公司的帕洛阿托研究中心(PARC)的 Van Jacobson 等提出的内容中心网络，简称 CCN(Content Centric Networking)。

8.1.2 移动优先

移动优先(MobilityFirst)项目主要考虑移动问题，该体系结构使用普遍的延时可容忍网络 DTN(Delay-tolerant Networking)提供鲁棒性，再结合自认证公钥的使用，就可提供一个具有天然可信任属性的网络。把移动作为第一属性，使得环境和位置感知服务自然地适合于该网络。该项目集中在移动、可扩展性和公平使用网络资源之间的

权衡,实现移动终端间的有效通信。

8.1.3 星云网络

星云(NEBULA)项目针对当前的存储、计算和应用都迁移到了“云”上这个事实,它把云计算的数据中心作为主要的数据仓库和主要的计算场所,数据中心被高速的、可靠的和安全的骨干网连接。该项目集中在部署云计算网络服务,使新的可信数据、控制和核心网络支持持久可用,从而实现一个可以快速提供计算服务的云计算基础设施。

8.1.4 可表达的架构

可表达的框架(expressive Internet Architecture,XIA)项目主要针对的问题是网络使用的多样化、可信通信的需求以及同时提供网络服务的利益相关者在不断增长。XIA 是一个可信的并可演化的体系结构。XIA 天生支持多个第一类责任者(x-centric),也支持未出现的应用模式,即 XIA 的体系结构可以随着网络背景和应用的变化而演化。XIA 创建了一个单一网络,在当前主要的通信主体(主机、内容、服务以及未来不可知的应用)之间提供固有的通信支持。

8.1.5 可选择的架构

可选择的架构(ChoiceNet)项目旨在开发一种新的未来网络架构设计,使用经济学的原则使得在网络的核心持续创新。这个新的网络体系结构的核心思想是支持的选择(Choice)。建立在这些原则的网络将能够适应当前和未来的挑战,提供新兴应用的解决方案。网络架构的设计和实现这项工作的目的是:①鼓励提供替代方案,让用户可以从一系列服务中进行选择;②让用户投票,用自己的资助,奖励卓越和创新的服务;③提供机制随时了解可用的各种替代方案的工作状态和它们的性能。从不同的学术方向提供 ChoiceNet 的解决方案,反映了跨学科专业知识交叉,包括计算机网络、网络系统、管理科学和网络经济学等。

8.1.6 面向服务的架构 SOFIA

由中科院牵头实施的面向服务的未来互联网体系结构(Service-Orientated Future Internet Architecture,SOFIA)借鉴了当前互联网参考模型 TCP/IP 分层和“细腰”模型的设计思想,但“细腰”向 OSI 参考模型的上层移动,服务标识成为新的“细腰”,彻底改变了 TCP/IP 以主机为核心的设计理念。以服务为核心的 SOFIA 体系结构顺应了互联网的应用场景,网络将具有更多的智能,标识和地址也将分离,而安全将成为体系结构内嵌的功能。这些设计理念和技术为解决 TCP/IP 体系结构面临的扩展性、动态性以及安全性问题,提供新的思路和理论基础。

8.2　信息中心网络

信息中心网络（Information Centric Networking，ICN）就是网络中的一切都可以看作是信息，可以说是一个信息互连的网络，而非主机互连，其核心对象是信息，通过信息的名字标识每一条信息。对网络来说，其中流动的都是有名字的信息，网络能区别每一个信息，但具体信息意义，网络并不知道，靠信息生产者和消费者的上层应用解释。整个网络及其终端就在各种信息的驱动下运行起来了，而网络的作用就是管理所有信息的流动和缓存，并用正确的信息快速响应信息的请求者。用户或应用可以只关注信息本身，而不关心信息块的其他属性，比如不用关心信息的所有者属性。

信息中心网络的设计与架构，主要针对当前 TCP/IP 互联网的可扩展性和有效的内容分发问题，该问题前几年已经引起了覆盖网（Overlay Network）和内容分发网络（Content Delivery Network）的研究热潮。经过多年的研究，P2P 和 CDN 在解决内容分发问题时仍存在一些安全性与可扩展性等不足。信息中心网络的解决方案，针对的是整个网络体系结构，其目标不只是解决内容分发问题，而是要解决当今互联网存在的所有问题。已有研究证明了信息中心网络能够更好地解决当今互联网中存在的各种问题。

在众多的信息中心网络中，施乐公司的帕洛阿托研究中心（PARC）的内容中心网络具有更多的优势，也是目前研究较多的体系结构，并且有开源的原型实现支持。NDN 项目便是在 CCN 基础上进行研究的。另外，欧洲的 CONNECT 项目也为完善 CCN 做出贡献，CONNECT 主要研究 CCN 的流量控制、命名、路由和转发，并思考 CCN 的部署策略。CONNECT 项目也通过一些网络服务和应用的案例，力求从经济上说明 CCN 取代当前互联网的不可抗拒的优势；另外，CONNECT 项目也开发一些模拟和仿真工具，用来测试和证明新的 CCN 协议的有效性。

8.3　软件定义网络

传统的网络设备，如交换机和路由器，都是基于专用的高性能硬件，完成网包的高速转发功能，缺乏灵活的重配置编程能力。这些网络设备一般只有少数几家厂商能够提供。随着通用多核处理器的发展与网络接口技术，网络接口向千兆/万兆以太网逐步过渡，PCIe（PCI express）的 I/O 技术得到了改进，并且内存速度也不断提高。网络处理能力显著增强，并具有灵活编程的能力。这些技术进步使得采用通用平台构建千兆/万兆交换和路由设备已经成为现实，而基于 Cluster 模式甚至可以达到 100Gbps 规模。这些通用平台一般采用通用的多核服务器，易于配置升级，运行常用的操作系统。

软件定义网络（Software-defined Network）就是用网络可编程性改变网络管理维

护难，配置复杂，支持应用不灵活等问题。

SDN 通过 OpenFlow 协议来控制交换机流表设置，所有的配置均可在控制器上用程序控制。一种典型的 OpenFlow 部署图如图 8.1 所示，图中所有的交换机与无线接入点都是实现了 OpenFlow 协议的，并且都受控制器的控制。目前软件定义网络在数据中心、云计算虚拟化中已经得到了应用。

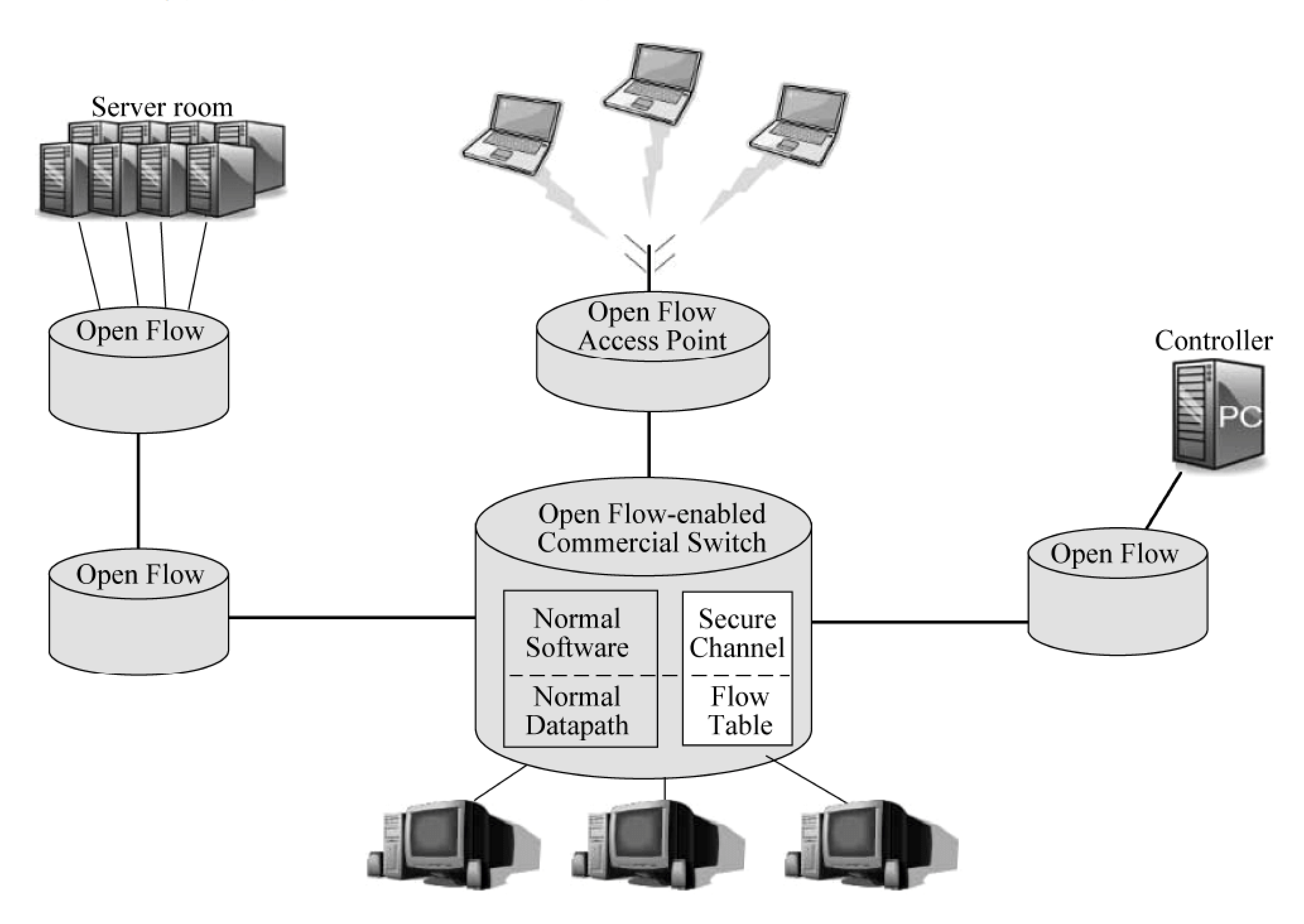


图 8.1　OpenFlow 交换部署图

第9章　网络安全研究

网络安全与网络架构是密切相关的两个领域，新的网络架构均视网络安全为必要条件。除了未来网络架构和传统的网络研究领域外，还包括虚拟密码货币和网流归档等新兴领域。

9.1　密码货币

9.1.1　虚拟货币

虚拟货币又称为电子货币（Virtual Currency 或 Digital Currency），在互联网进入高速发展之前，只存在于人们的各种单机游戏中，通过打怪、任务等方式，主角在游戏中积累财富，用以购买游戏中的各种道具，跟现实并未发生直接的联系。自从互联网将门户、社区和游戏进行互连，各种论坛、网游中的虚拟货币变得在玩家之间可以进行交易，从而形成了一种新的金融市场，这种类型的虚拟货币更趋向于以各种网络游戏币交易为主的庞大产业链。

另一种虚拟货币可以理解为是互联网公司发行的专用货币，用以购买该公司所属的各种互联网服务。腾讯公司的 Q 币是一个典型的例子，可用来购买会员资格、QQ秀等增值服务。另外，京东的京豆、百度的百度币、淘宝的淘金币均属于此种类型的虚拟货币。这种类型的虚拟货币根据其获取的方式以及难易程度不同，所能应用的领域也有所不同。

9.1.2　比特币原理

比特币（bitcoin）是具有真正货币体系的一种分布式虚拟货币。比特币是由中本聪在 2007 年发表的论文 *Bitcoin：A Peer-to-Peer Electronic Cash System* 所描述的。它与各种游戏无关，与各大互联网公司也无关，这种虚拟货币采用的是密码学的原理，通过分布式机制进行发布，拥有类货币的属性，所以又称为密码货币（Crypto-Currency）。以比特币为例，由于炒作等因素，比特币在 2013 年价格达到了顶峰。以比特币为首，一大批类似的虚拟货币也被相继开发出来。在虚拟密码货币的世界里，流行着“比特金、莱特银的说法。

比特币是一种开源的 P2P 软件产生的电子货币，不依靠特定货币机构发行，而是通过特定算法（哈希运算）大量计算产生，其流通方式是使用 P2P 网络中的节点构成分布式数据库来确认和记录所有的交易信息。P2P 网络的去中心化特性与算法本身可以确保比特币稳定的发行速率。

比特币运用了包括数字签名、公私钥加密系统等多种算法来确保交易安全性。同时比特币作为一个去中心化的系统，数以万计的矿工通过挖矿的方式来进行记账，使得比特币能够在没有一个中央银行系统的情况下维护交易记录以实现交易的进行。同时为了对参与记账的矿工进行奖励，比特币通过计算满足特定条件的账单哈希值的方法来作为工作证明，对计算出来的矿工给予比特币的奖励，这一机制调动了矿工的积极性，保证了交易能够通过账单的方式得到确认。

传统的货币是由各国的中央发行机构统一、集中发行的，而比特币不依赖于特定的中央发行机构，P2P 的分布式特性与不存在中央管理机制的设计确保了任何机构都不可能操控比特币的价值，或者制造通货膨胀。其主要特点如下。

(1) 去中心化。比特币是一种分布式虚拟货币，由分布式的用户组成网络，没有中央银行。

(2) 全世界流通。任何人可以在任意一台接入互联网的计算机上挖掘、购买、出售或收取比特币。

(3) 专属所有权。操控比特币需要 P2P 用户的私钥，公钥作为用户身份标识和钱包地址。

(4) 低交易费用。汇出比特币是免费的，确保交易更快执行则需支付 1 比特分。

(5) 无隐藏成本。只要知道对方比特币地址就可以进行有效支付。

(6) 跨平台挖掘。用户可以使用各种具有强大计算能力的硬件设备进行比特币的挖掘。

虽然比特币不会被中央机构操控价值，但是其价格可受庄家的人为控制，并出现大起大落的情况，经过 2013 年的火爆，比特币本身的货币属性正在被各种炒作比特币的人群所消费殆尽，现在的比特币更像是一只采用了先进密码学技术的股票，但不可否认的是，这种将密码学与分布式网络的结合的确创造了一项潜力无限的新技术，启发人重新思考金融里的“必然之物”。

9.1.3 比特币定价

许多面向科技玩家的网站，已经开始接受比特币交易，包括火币网、BTCChina 之类的网站，以及淘宝某些商店，甚至能接受比特币兑换美元、欧元等服务。毫无疑问，比特币已经成为真正的流通货币。但是比特币的价格在波动，似乎捉摸不透。

主流经济学家开始研究分析比特币。早先，这些分析总是集中在比特币的安全性。而现如今的分析总是集中在比特币能否成为未来的主流货币，而这其中争论的焦点又往往集中在比特币的通缩特性以及内在价值上。

围绕着比特币等虚拟货币的价值以及价格问题，产生了不同学派的经济学家。凯恩斯学派的经济学家们认为政府应该积极调控货币总量，用货币政策的松紧来为经济适时地加油或者刹车。而奥地利学派经济学家认为政府对货币的干预越少越好，货币总量的固定导致的通缩并不是很重要，甚至是社会进步的标志。

因此深入研究比特币等虚拟货币的定价以及影响其价格的因素变得尤为重要。在

研究比特币价格理论方面，意大利人 Gbianchi 做出了重要贡献。他的研究 *A Bitcoin Price Theory Proposal* 发在 bitcointalk 上。后来，该成果被翻译成英文，成为继中本聪创建 BTC 以来最好的对价格相关分析的论文。

近年来，比特币、莱特币等虚拟货币纷纷涌现，也有许多的研究人员投入到对虚拟货币的研究。但是对比特币等虚拟货币的研究还处于发展阶段，还未非常成熟，有许多方面可以发掘深究，特别是比特币等虚拟货币的定价理论模型。这对于将来更好地把握虚拟货币价值趋势有非常重要的意义。

9.2 网流归档与检索

9.2.1 网流归档系统

随着互联网应用的普及和移动无线网络的大规模商用，海量信息内容极大丰富了用户。而移动互联网的爆发，使得用户可以从任何地方、任何时间访问网络上的任何内容，产生更为丰富的流量数据。整个互联网流量保持着高速增长，任何一家大型互联网公司在日常运营中生成和累计的用户流量数据都是相当庞大的，以至于不能用千兆(Giga，G)或万亿(Trillion，T)级字节的数据来衡量。思科公司报告预言，互联网流量数据在 2011—2016 年之间将增长 4 倍，于 2016 年达到 1.3 ZB(Zetta，十万亿亿字)。互联网流量数据是一种典型的流式大数据。

网络安全问题日益凸显，由于其开放性，计算机网络要遭受大量可知或未知的攻击。在这种背景下出现很多网络安全防范技术，如入侵检测系统、特征码检测、安全扫描技术等，但是很多攻击是无法进行及时检测和预防的，需要通过对网包的捕获来实现对网络流量信息的收集，便于以后的分析和使用。攻击不可避免，总有防不胜防之处，如何回溯追踪是一个很重要的问题。

网络监控一直是网络业务管理、网络故障诊断与网络安全的核心功能。除了实时的防火墙和入侵检测系统之外，网流归档系统是网络防护体系的重要补充。

网络的日益发展带来网络流量的剧增，其中隐藏了大量可用信息，特别是针对网络安全中可知或未知的攻击。很多攻击是无法进行及时检测和预防的，这需要通过对网包的捕获实现对数据信息的收集，便于以后的分析和使用。网络监测一般分为两种，一种是实时监测，即实时捕获和检查，在检查完之后，直接丢弃包的头部和负载，如 TelegraphCQ、Gigascope 等；另一种不仅具有对数据进行线速捕获的功能，还具有存储、回溯查询和高效检索数据等其他功能，如 NET-FLi、NetStore、Hyperion 等。上述系统中大部分都以 flow record 的格式输入，相比于 packet 形式，简化操作，保护隐私。

9.2.2 网流归档的关键技术

1. 高性能网包/流获取技术

互联网流量的数据一般特点是数量巨大，到达速度快。以 10Gbps 链路为例，如果

按每个网包 64B 计算，每秒将达 1400 万网包，即使经过聚合，也会有多到几十万至上百万的流记录。即使只处理网流数据，一个运营商的一个核心点每秒产生的网流记录可达上万条，每日的上网记录数据生成量超过 300 亿条。

因此，如何实时获取和存储高速到达的网包和网流是一个挑战性问题。

2. 高性能网包/流存储技术

传统的网包和网流记录采用关系型数据库以行记录的方式存储，这种方式存在存储空间消耗巨大，检索速度慢的缺点。目前，为了有效存储网包/流信息，按列存储及压缩是一种节省存储空间开销的方法。对网流信息一般采用通用的 LZO 压缩方法，或者使用根据流信息优化的新型方法，如 RasterZip、BreodZip。

3. 高性能索引技术

为了检索如此巨大的数据，需要创建高效的索引(Indexing)。倒排索引是通用数据检索技术，广泛应用于文本检索，如搜索引擎。但是对于网流的查询，主要是对数值进行检索，倒排索引并不是最有效的方式，位图索引是检索数值的高效方式。

检索如此巨大的数据，为此需要创建巨量的索引，这就是“索引空间”爆炸问题。即使像谷歌这样的大公司，也一直非常重视对索引空间的压缩。为了高效地存储索引并在检索时装载入主存储以加快检索查询速度，一般会对索引空间进行分段，同时对索引文件进行有效的压缩。位图编码算法就是针对位图索引的有效的压缩方法，也是解决索引空间爆炸问题的关键所在。

9.3 同态加密

9.3.1 隐私保护

当前，互联网用户在使用 Web 服务时，往往会泄露个人的隐私。例如，使用谷歌进行关键词搜索时，你的关键词直接暴露给谷歌；又比如你享受云计算的效率时，你的数据也完全暴露于云端服务器。现在，随着同态加密技术的发展，用户可以在获得服务的同时可以保护隐私。

考虑两个百万富翁想比较谁更有钱，但又不想透露自己钱的数额。再考虑一个匿名的投票系统，投票方、计票方、宣布方三权分立，采用公钥加密，只有宣布方拥有私钥。投票方将用公钥加密后的票送到计票方，计票方对加密后的票进行统计，得到汇总的结果，宣布方拿到该结果后解密之，即得总票数。宣布方不知道单独每张票的情况，从而实现了匿名；计票方解不出票面信息，于是可以防止计票方从中作梗。类似的问题有很多，我们需要将解决问题的多个步骤托管给第三方，但同时又不想透露问题的具体细节。

9.3.2 同态加密

同态是抽象代数中对于两个代数结构保持结构不变的映射的描述。相应地,同态加密就是特定的从明文空间到密文空间的映射,使得明文空间的代数运算与密文空间的代数运算等价。随之而来的优点是在明文空间的任何代数运算等价于将明文空间通过加密函数映射到密文空间后,接着进行相应的代数操作,最后使用解密函数映射回明文空间。如果同态加密的加密体系是安全的,那么如果我们把运算的第二部分,也就是在密文空间的计算托管给第三方,不会造成明文的泄露。除了安全性,同态加密必须保证有效性,所有相关操作的计算复杂度应该在多项式范围内。

注意以上对同态的定义符合我们刚才提出的用户隐私保护的需求,解决问题的部分被安全地托管到第三方。

满足同态加密的算法很多:ElGamal 满足乘法同态,GM 和 Paillier 满足加法(异或)同态等。注意到为了解决之前匿名的投票系统的问题,我们只需要使用一个加法同态的算法。但如果现在操作更加复杂,比如说我们要将文件保存在云端,然后要服务器检索文件,把所有包含"全同态"的文件列出来,这显然不是仅仅通过一种运算就可以解决的。由于任何算法都可以看成一个由加法和乘法组成的布尔电路,如果有一个加密方案能够同时满足对加法和乘法同态,并且满足有效性和安全性,那么这个算法就可以用来实现所有计算的托管,也就满足了之前的所有需求。人们称这样的加密方案为全同态的。

一个安全的适合第三方托管的加密方案应该满足"电路保密性"和"紧凑性","电路保密性"指第三方的运算电路对于其他任何一方都是保密的,"紧凑性"是指反馈的密文的长度与第三方的运算电路无关。全同态加密能够同时满足"电路保密性"和"紧凑性"。

9.3.3 研究发展

在 Rivest 等人提出 RSA 算法后不久,Rivest 又引入了同态加密的概念。RSA 算法本身满足乘法同态,而当时并没有证明全同态加密的是否存在。此后,一系列的论文研究试图解决这一问题。

2009 年,Gentry 形式化地提出了第一个全同态加密方案。并给出了基于理想格构造,在理论上解决了这一问题,但是实际的效率并不高。之后,一系列的改进措施被提出,简化了全同态加密方案中的公钥以及密文。

2010 年,Dijk 等人给出了 Gentry 基于理想格的方案在整数下的描述。另外,Gentry 也证明了通过适当的方法生成密钥的安全性可以在量子上降低到理想格中格的难度的最差情况。同年,Smart 和 Vercauteren 基于格的"主理想"首次实现了 Gentry 提出的全同态加密方案,此方案的私钥为单整数,在参数极大的情况下的 squash 过程不能有效完成。

2011 年,Gentry 实现了理想格上的全同态加密的变种,并对各个环节进行了优化,

虽然复杂度很高，但速度已经在实验接受的范围之内，不过离实际需求的距离仍然遥远。随后，Gentry 又构造了不需要 squash 过程的一个全同态加密方案，由于 squash 过程是全同态加密中最费时的过程，不需要 squash 的方案将会大大简化全同态加密，使之能够更贴近应用。紧接着 Gentry 还构造了不需要进行“可启动化构造”的方案，这为全同态加密的方案设计又提供了一种新的思路。

以上两种改进都是基于格的构造。

9.4 加密数据库

因为攻击者可以利用软件的漏洞以非正当途径获得数据库控制权限以及数据库管理员可以看到数据库的内容，网上的应用程序对于重要数据的保护面临着巨大的挑战。例如，近期引起很大风波的 CSDN、天涯等网站用户信息泄露等。其中最有代表性的就是 CSDN 的密码泄露事件。2011 年 12 月，CSDN 的安全系统遭到黑客攻击，600 万用户的登录名、密码及邮箱遭到泄露，更致命的是，用户泄露的密码竟然是以明文方式泄露。2014 年，网上火车票订购 12306 网站泄露大量用户名与密码。虽然此次失窃的只是密码集，用户只要及时修改密码即可避免隐私失窃，但用户修改密码只是“治标”，网站改变数据存放策略才是“治本”。

减少因为服务器被攻击而引起的危险的一个有效的方法就是对重要的数据进行加密。现在有很多算法实现了这个思路，比如说 SUNDR、SPORC and Depot 等。但是很多重要的应用软件，甚至是以数据为基础的网页，都没有运用这个思路，因为这样做有一个比较大的问题就是把现在已经存在的服务端应用软件改成可以实现这些算法需要特别大的工作量。

9.4.1 CryptDB 设计

美国麻省理工学院的 R. A. Popa 等提出了 CryptDB，它允许用户查询加密的 SQL 数据库，在不解密储存信息的情况下返回结果。密码专家长期以来一直在寻找实现全同态加密的方法，也就是数据加密成难以破译的数字字符串，能对这些加密后的字符串进行数学处理，然后解密结果。但目前的全同态加密方案存在实用性问题，耗费的计算时间太长。CryptD 首次解决了目前实用问题，它将数据嵌套进多个加密层，每个都使用不同的密钥，允许对加密数据进行简单操作。此前的全同态加密方案加密数据操作所增加的计算时间是数以万亿倍计的，而 CryptDB 只增加 15%～26%。

CryptDB 所做的工作实际上就是在现有的 DBMS 上添加了一层接口，使得数据库中存储的是加密后的数据，并且能够支持在加密数据上进行 SQL 查询。下面介绍我们了解到的一些情况。

1. CryptDB 的应用目标

服务器被攻破是指由于数据库中的信息未加密带来的用户信息泄露安全问题。

CryptDB 为此对数据库中的数据进行加密。

Arbitrary Threats 这类威胁主要担心攻击者能够访问 keys 造成的安全问题。CryptDB 为此对不同的数据项(Data Items)(如不同用户的数据)使用不同的 key。

2. CryptDB 的整体结构

CryptDB 的整体结构如图 9.1 所示。

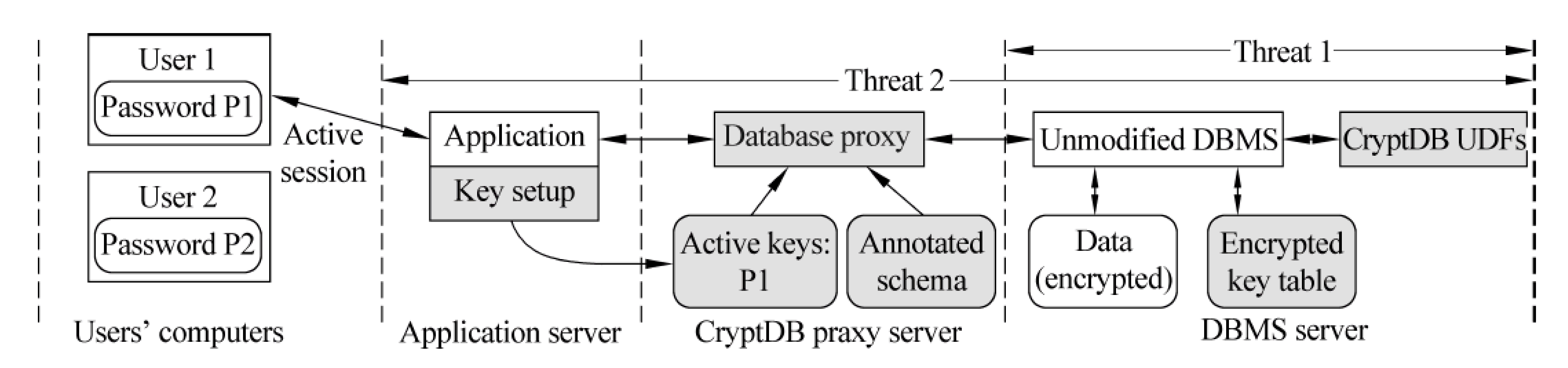


图 9.1 CryptDB 的整体结构

灰色部分是 CryptDB 相关的,可以看到,它覆盖了 Application Server、CryptDB proxy server、DBMS server 三个层次,但是主要在 CryptDB proxy server 这一层。也就是说,CryptDB 对现有的应用程序、数据库管理系统的变动并不大,主要就是在它们中间增加了一层,使得数据访问存储都加密了,更加安全一些。另外两层的变动较小,数据库方面主要是利用数据库本来支持的 UDF(User Defined Function)来实现功能,而 Application 层也只要对相应用户进行 Key setup 即可。

3. CryptDB 的优势

CryptDB 还有一个比较大的优势在于现在的 SQL 只需要更改特别少的代码就能够运行 CryptDB,而且根据有关实验表明,CryptDB 的 3 个应用实例 phpBB、HotCRP、grad-apply 均体现出了其高效性。

同时我们也研究了 CryptDB 所支持查询的过程以及实现的算法,简单来说,CryptDB 为不同类型的 SQL 查询设计了一些加密方法。

(1) Random(RND),使用一个辅助列进行加密。

(2) Deterministic(DET),使用相同方法加密,保证一样的原文加密后得到一样的密文,支持 GROUP BY、COUNT、DISTINCT 等操作。

(3) Order-preserving encryption (OPE),特殊的一类加密方法,加密前后保持数据顺序,用于支持 ORDER BY、MIN、MAX、SORT 等操作。

(4) Homomorphic encryption (HOM),目的是支持对数据的运算,加密前的运算可以变为加密后的另一种运算,用于支持 SUM 等,实现时将 SUM 替换为 DBMS 中的特殊 UDF。

(5) Join (JOIN and OPE-JOIN),支持不同类型的 JOIN 操作。

(6) Word search (SEARCH),用于支持在原文中搜索(LIKE 操作),大概方法是

提取关键词,然后加密。

CryptDB 里面涉及一个重要的思想是 Onion 结构,具体如图 9.2 所示。

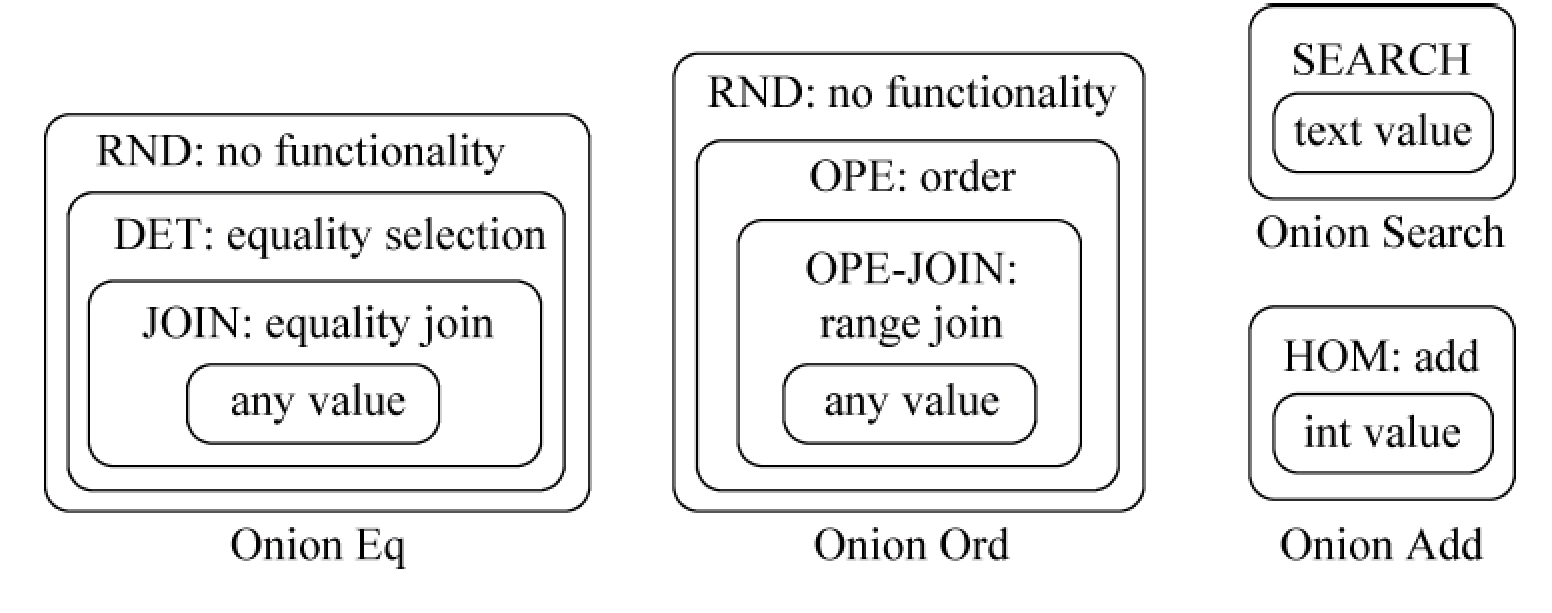


图 9.2　Onion 结构

数值 value 是指原文经过多层加密存储的是较为安全的数据,对于不同类型的操作,需要进入某一层,比如一个 equality join,需要用 Onion Eq 进入到第二层,支持 JOIN 的那一层。

对于原本数据库的每一列,会被拆成多列,以支持各种类型的操作(如果应用层只会用到其中某些操作,则可对数据库进行简化)。

通过对 CryptDB 的研究与实验,CryptDB 确实允许用户查询加密的 SQL 数据库,在不解密储存信息的情况下返回结果。同时 CryptDB 对于每个数据都使用不同的密钥,并且密钥与用户名、密码相关,允许对加密数据进行简单操作。并且,CryptDB 花费的时间在可接受范围之内。

9.4.2　用户信息托管

根据 CryptDB 的原理,为了实现数据库内容加密,同时还有效利用已有的数据库接口,解决办法是使用数据库代理。用户对数据的访问先经过代理,再由代理与数据库交涉。这里用 PHP 实现了一个简单的加解密数据的代理。

用户一旦登录,服务器端就会保存一个包含用户名和密码的 Session,直到用户退出。对于用户存数据的操作,首先数据被服务器传给代理,代理先随机生成一个串作为 Salt,理论上应该为数据库表的每个字段生成一个 Salt,但是这里为了简单起见,一行数据共用一个 Salt。将用户名和密码与这个 Salt 作用生成一个 key,用这个 key 作为密钥对这一行数据进行加密,将加密结果以及 Salt 值作为一行存入数据库。加密方法使用 Rijndael 算法。数据加密的过程如图 9.3 所示。

用户个人信息在数据库中的内容如图 9.4 所示。

因为密钥的生成需要数据所属用户的用户名和密码,所以即使攻击者拿到数据库,也无法获知用户存储的数据。引入 Salt 的原因是防止攻击者通过使用彩虹表(Rainbow table)一类的预计算表反向破解。

对于取数据的操作,代理首先在表中查找获得所有属于该用户的数据行,并得到该行的 Salt,逐行解密,将解密出来的键值与用户查询的键值对比,相等则返回查询结果。

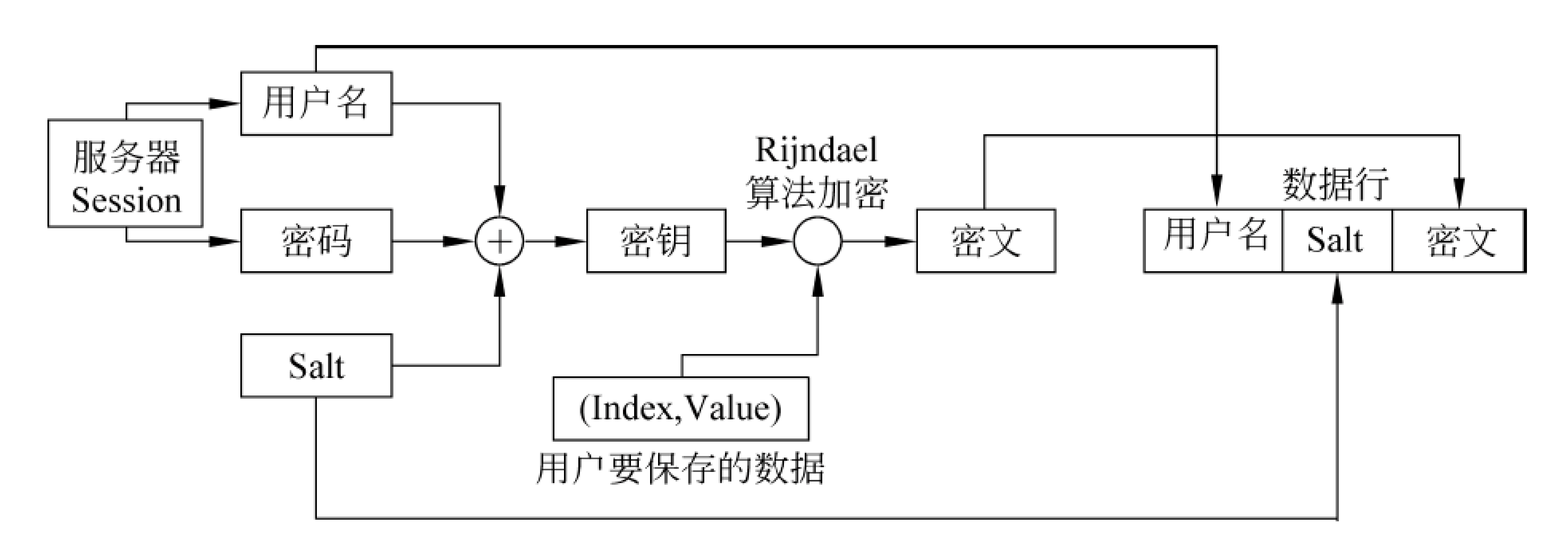


图 9.3 数据加密的过程

user	site	value	syskey
64489c85dc2fe0787b85cd87214b3810	Y8THzeAtI44LHpZya8LvsB9I6fr/12/L13i11I6JGCE=	gmCtW20gBbI8F0/sGe00xz/mCsLUMwxtX67delpl1Dw=	21MXEvWRaxkpcFyB8fMF
64489c85dc2fe0787b85cd87214b3810	Frpaxe0lwDCMvZL4ysOV5hX3viJIOa4uXkj2+ljH3AY=	ABZT7tcyuJ0WwoV3LKMmOJQVsx8kYG5GWGAdhQyFfQ=	8JENlxl9OImjaxkDo1yzkh0
64489c85dc2fe0787b85cd87214b3810	OsKSv/pZE2eOa/X4vTNRzfKmzbgWt7JqRKTWfNeaC8M=	MybrTwQo1GXFSkZ3J7q0Amt1YLbrAvBG4gAafhNAJuQ=	TuJOhYJOVuHWb0JETeler
64489c85dc2fe0787b85cd87214b3810	TCDi3cxFRRaefe3rnLu/4WJdR/aURBY9IskN+a/g3tU=	e7Konz+Adk+XTo7YIGeyJKeqB7cATEHxRBkzD6W4fag=	7WVcpi9YzgIKbkjcNQdqJ2
64489c85dc2fe0787b85cd87214b3810	wUg0Dq/THBR469tLxGe1LIJJG88x59WBFGxSYiL4t+4=	mm9nID0ddyhA9hbNPaiX98v1nSW7LeUWCdL7vX/YMIg=	W5kLWtApQ9MnAr85Qj2L
64489c85dc2fe0787b85cd87214b3810	QSwH8I+82fqPfNOduDwloNy1tfoHjWsdLe0TS/6e1OY=	mU7otSRVXWIIb+P81Zb/a2U/p57AelcMuCjR0b91SGs=	kn0ZuNyzUZQzmDUIoR8p
64489c85dc2fe0787b85cd87214b3810	m3vWw9FSBbNsvWeZZBtOeRm85Jp43kg1xWI49oajFj8=	LKL+hgyEx5RL+HJkeJptBQK0L6bFRUo10CJFSRPiQIU=	Sr2tO9cdMxejsPYfGL0B4N

图 9.4 数据库中的内容

解密过程如图 9.5 所示。

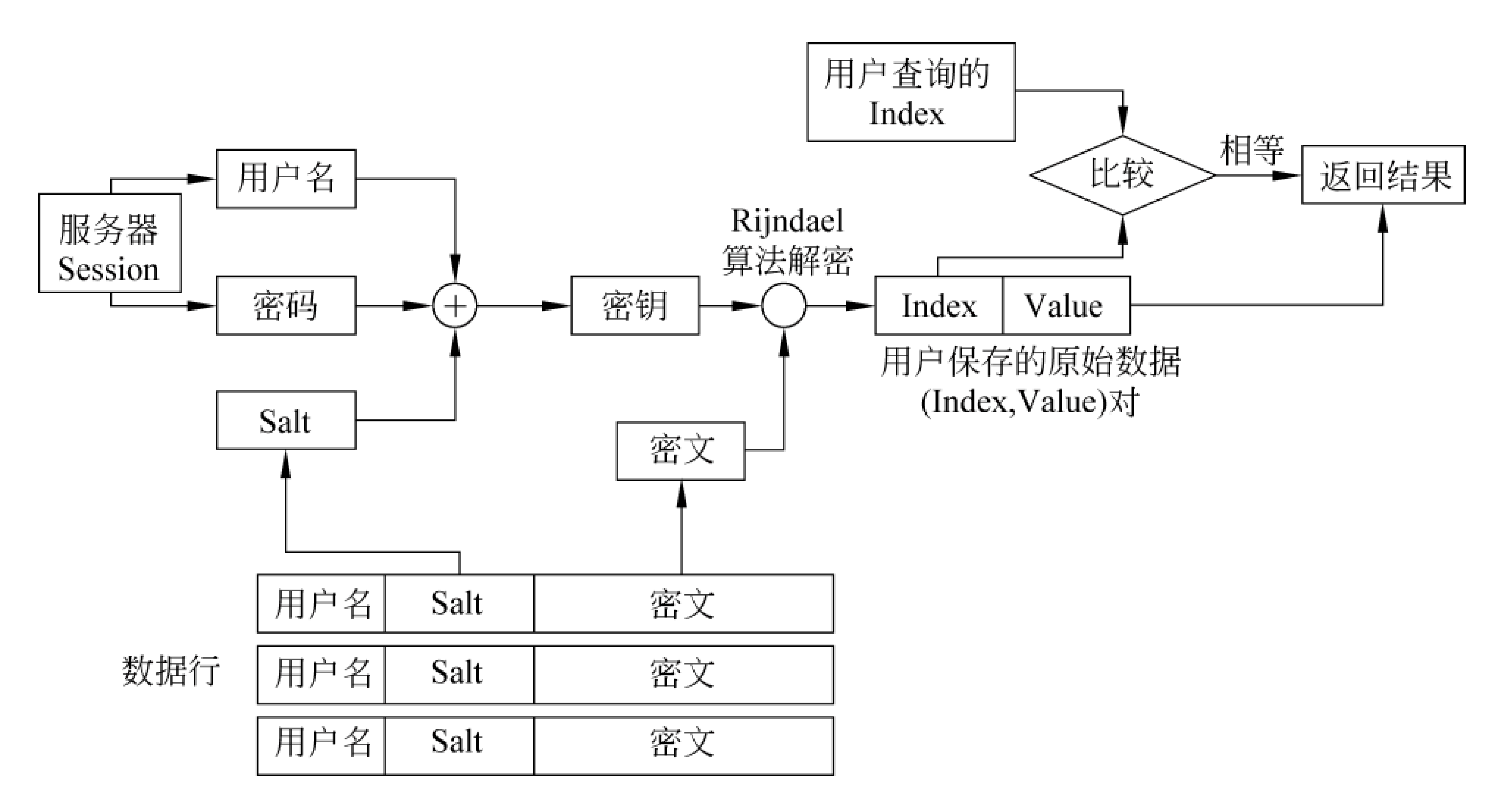


图 9.5 解密过程

9.5 密文检索综述

9.5.1 加密数据的线性搜索技术

加密数据线性搜索技术是由加州大学伯克利分校的 XiaoDong Song、David Wagner 和 Adrian Perrig 等人在 DARPA(美国国防部先进研究项目局)的资助下研究完成的,用于保护美国政府核心数据。该技术是可证明安全的,同时还是实际有效的加

密数据检索方案。主要包括基本方案、可控搜索方案、支持隐藏搜索方案和最终方案。

基本方案描述如图 9.6 所示，Alice 将要加密的每篇文档分为一系列的单词序列 W_1、…、W_l。为了加密长度为 n 的单词 W_i，Alice 使用伪随机数函数 G 产生 n-m 长度的随机数 S_i，对单词 W_i 都给定一个密钥 K_i，S_i 通过 F 函数在密钥 K_i 作用下产生 m 长度的乱数$F_{K_i}(S_i)$，与 S_i 共同组成长度为 n 的乱数 $T_i:=\langle(S_i),F_{K_i}(S_i)\rangle$，然后将 W_i 与乱数 T_i 模 2 加输出密文 C_i，Alice 将 C_i 发送给 Bob 存储。为了检索明文 W，Alice 需要告诉 Bob 的内容包括 K_i 和明文 W，其中 i 为 W 可能出现的位置；然后 Bob 通过计算获取$\langle(S),F_{K_i}(S)\rangle:=W\oplus C_i$，然后只需要通过 S 和 K_i 计算获取 $F_{K_i}(S)$与 $F_{K_i}(S_i)$比较是否相等即可实现对单词 W 的检索。在本方案中，Alice 要么告诉 Bob 单词 W 可能出现的位置 i，要么告诉 Bob 所有的密钥 K_i，这显然不能满足用户要求。

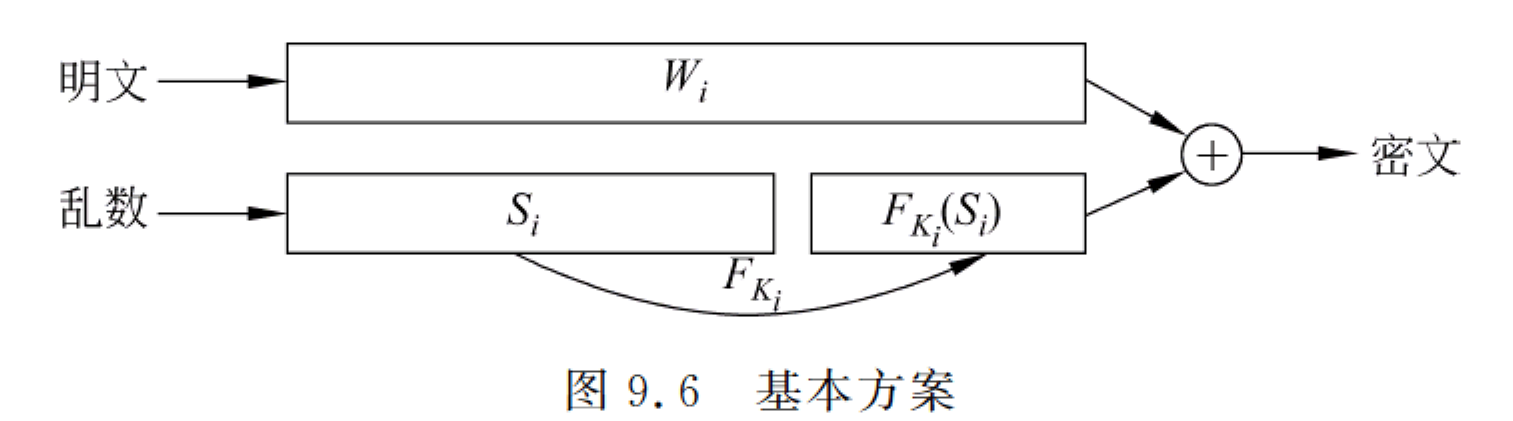


图 9.6 基本方案

可控检索方案在基本方案的基础上改进了密钥 K_i 的产生方式，使 $K_i:=f_{K'}(W_i)$，其中 f 为 MAC 函数，只需要告诉 Bob 单词 W 和 K_i，而不需要暴露 K'，这样只有出现 W 的地方才会暴露明文信息，而其他地方不会暴露任何信息，这仍然不能实现加密检索。

支持密文检索的方案是在可控检索方案的基础上，先将文档的每个单词 W_i 使用 ECB 方式加密或者是固定 IV 的 CBC 模式，密钥为 K''，加密函数为 E，加密得到 X_i，对 X_i 按可控检索方案处理，这样为了实现检索 Alice 只需要提供 $X:=E_{K''}(w)$和 $f_{K'}(X)$。然而，此方案还存在一个问题，如果 $K_i:=f_{K'}(X)$，那么 Alice 在只知道密文的情况下只能根据伪随机数函数 G 产生 S_i，此时由于 Alice 还不知道 X，所以也无法根据公式求出 K_i，也就无法获取 $F_{K_i}(S_i)$，从而无法实现解密。

最终方案就是在密文检索方案的基础上将 X 分成左右两个部分 $X:=\langle L_i,R_i\rangle$，其中 L_i 的长度就是 S_i 的长度，K_i 的产生变成 $K_i:=F_{k'}(L_i)$这样，Alice 在获取到密文后，通过伪随机数函数 G 产生 S_i，利用公式 $L_i:=S_i\oplus C_i$，再求取 $K_i:=f_{k'}(L_i)$，从而 $R_i:=F_{K_i}(S_i)\oplus C_i$，最后将 L_i 和 R_i 合并经过解密函数 D 即可实现密文的解密。

9.5.2 基于 Bloom Filter 的安全索引算法

Bloom Filter 算法的基本原理是采用包含 m 位的位数组存储，将 n 个元素集合 $S=\{x_1,x_2,\cdots,x_n\}$用 k 个相互独立的哈希函数映射到$\{1,2,\cdots,m\}$的范围中，如图 9.7 所示。其核心思想是利用 k 个不同的 Hash 函数来解决 Hash 冲突问题，其优点是空间效率和查询时间都远远超过一般的算法，缺点是存在一定的错误率，且索引删除困难。当要查询单词 w 的时候，计算 w 的 k 个不同的 Hash 值，如果结果所在的位均为 1，表

示查询结果在集合 S 中，该算法的错误率为

$$f = (1 - e^{-kn/m})^k = (1 - p)^k$$

实际使用时的 Hash 算法有 Jenkins 算法、Spooky 算法和 Murmur 算法等。

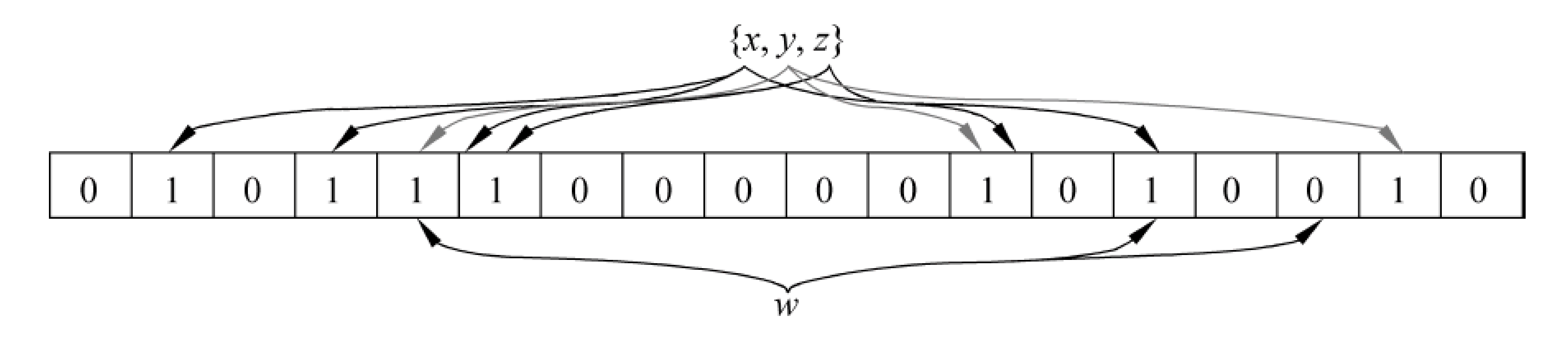


图 9.7　Bloom Filter 算法原理

IND-CKA 和 IND-CKA2 安全索引算法的核心思想就是在 Bloom Filter 算法的基础上，将 k 个 Hash 函数替换成一组带密钥的安全 Hash 函数(例如 HMAC-SHA1)，从而来抵御选择明文攻击，来实现安全索引 Z-IDX。因为文件内容建立索引后，不需要访问文件内容，所以安全索引方法很自然地就能支持基于线性搜索的密文检索方法

参 考 文 献

[1] 詹姆斯·格雷克.信息简史[M].高博译. 北京：人民邮电出版社，2013.

[2] 约翰·麦考密克. 改变未来的九大算法[M]. 管策译. 北京：中信出版社，2013.

[3] 赵燕枫 . 密码传奇[M]. 北京：科学出版社，2008.

[4] 比尔·盖茨. 未来之路[M]. 辜正坤译. 北京：北京大学出版社，1996.

[5] 吴军. 浪潮之巅[M]. 北京：人民邮电出版社，2013.

[6] Brian W. Kernighan. 世界是数字的. 李松峰，徐建刚译. 北京：人民邮电出版社，2013.

[7] Paul Hoffman. IETF 之道，http:/www. ietf，org/tao-translated-zh. html.

[8] Fluhrer，S. ，Mantin，I. ，& Shamir，A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. In Selected Areas in Cryptography. Springer Berlin / Heidelberg.

[9] Tews，E. ，& Beck，M. (2009). Practical attacks against WEP and WPA. Proceedings of the second ACM conference on Wireless network security. ACM.

[10] Raluca Ada Popa，Catherine M. S. Redfield，Nickolai Zeldovich，and Hari Balakrishnan. CryptDB：Protecting Confidentiality with Encrypted Query Processing.

[11] R. A. Popa，N. Zeldovich，and H. Balakrishnan. CryptDB：A practical encrypted relational DBMS.

[12] Boldyreva，Alexandra，Nathan Chenette，Younho Lee，and Adam O' neill. "Order-preserving symmetric encryption." In Advances in Cryptology-EUROCRYPT 2009，224～241. Springer Berlin Heidelberg，2009.

[13] Boldyreva，Alexandra，Nathan Chenette，and Adam O' Neill. "Order-preserving encryption revisited：Improved security analysis and alternative solutions." Advances in Cryptology-CRYPTO 2011. Springer Berlin Heidelberg，2011. 578～595.

[14] J. Li，M. Krohn，D. Mazieres，and D. Shasha. Secure untrusted data repository(SUNDR). In Proceedings of the 6th Symposium on Operating Systems Design and Implementation，91～106，San Francisco，CA，December 2004.

[15] P. Mahajan，S. Setty，S. Lee，A. Clement，L. Alvisi，M. Dahlin，and M. Walfish. Depot：Cloud storage with minimal trust. In Proceedings of the 9th Symposium on Operating Systems Design and Implementation，Vancouver，Canada，October 2010.

[16] Song，Dawn Xiaoding，David Wagner，and Adrian Perrig. "Practical techniques for searches on encrypted data." Security and Privacy，2000. S&P 2000. Proceedings. 2000 IEEE Symposium on. IEEE，2000.

[17] Mihir Bellare，Roch Guerin，Phillip Rogaway，XOR MACs：New Methods for Message Authentication Using Finite Pseudorandom Functions (1995)，15 ～ 28，CRYPTO 1995，963，1995.

[18] Bellare，Mihir，Krzysztof Pietrzak，and Phillip Rogaway. "Improved security analyses for CBC

MACs." Advances in Cryptology-CRYPTO 2005. Springer Berlin Heidelberg,2005.

[19] Bellare,Mihir. "New proofs for NMAC and HMAC: Security without collision-resistance." Advances in Cryptology-CRYPTO 2006. Springer Berlin Heidelberg,602~619, 2006.

[20] NIST Computer Security Division's(CSD)Security Technology Group(STG)(2013). "Block cipher modes". Cryptographic Toolkit. NIST. Retrieved April 12,2013.

[21] Eu-Jin Goh, Secure Indexes. http://eprint. iacr. org/2003/216. Received 7 Oct 2003, last revised 16 March 2004.

[22] M. Bellare, R. Canetti, and H. Krawczyk. HMAC: Keyed-hashing for message authentication. RFC 2104,Internet Engineering Task Force(IETF),February 1997.

[23] Dr. Dobb's. Hash Functions and Block Ciphers. http: //burtleburtle. net/bob/hash/doobs. html.

[24] SpookyHash: a 128-bit non-cryptographic hash. http: //burtleburtle. net/bob/hash/spooky. html.

[25] General Purpose Hash Function Algorithms. http: //www. partow. net/programming/ hashfunctions/.

[26] SMHasher& MurmurHash3. http://code. google. com/p/smhasher/.

[27] R. Rivest, L. Adleman, and M. Dertouzos. On data ganks and privacy homomorphisms. Foundations of Secure Computation,1978.

[28] Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulars on ciphertexts. Lecture Notes in Computer Science,2005.

[29] C. Aguilar Melchor,G. Castagnos,and G. Gaborit. Lattice-beased homomorphic encryption of vector spaces. IEEE International Symposium on Information Theory,2008.

[30] T. Sander, A. Young, and M. Yung. Non-interactive CryptoComputing for $NC^ 1 $. Foundations of Computer Science,1999.

[31] Carlos Aguilar Melchor, Philippe Gaborit, and Javier Herranz. Additive Homomorphic Encryption with t-Operand Multiplications. IACR ePrint archive,2008.

[32] C. Gentry. Fully homomorphic encryption using ideal lattices. STOC,2009.

[33] D. Stehle and R. Steinfeld. Faster Fully Homomorphic Encryption. Asiacrypt,2010.

[34] N. P. Smart and F. Vercauteren. Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes. PKC,2010.

[35] Marten van Dijk and Craig Gentry and Shai Halevi and Vinod Vaikuntanathan. Fully Homomorphic Encryption over the Integers. Eurocrypt,2010.

[36] C. Gentry. Toward Basing Fully Homomorphic Encryption on Worst-Case Hardness. Crypto, 2010.

[37] C. Gentry,and S. Halevi. Implementing Gentry's Fully-Homomorphic Encryption Scheme. EuroCrypt,2010.

[38] O. Goldreich,S. Goldwasser,and S. Halevi. Public-key cryptosystems from lattice reduction problems. CRYPTO,1997.

[39] D. Micciancio. Improving lattice based cryptosystems using the hermite normal form. Lecture

Notes in Computer Science，2001.

[40] M. Dijk. Fully Homomorphic Encryption over the Integers. Crypto，2010.

[41] C. Gentry. Fully Homomorphic Encryption without Squashing Using Depth-3 Arithmetic Circuits. eprint. iacr. org，2011.

[42] C. Gentry. Fully Homomorphic Encryption without Bootstrapping. eprint. iacr. org，2011.

[43] F. Fusco，M. Vlachos，and X. Dimitropoulos. RasterZip：Compressing Network Monitoring Data with support for partial Decompression，IMC'，2012.

[44] G. Ma，Z. Guo，X. Li，Z. Chen，J，Cao，Y. Jiang，X. Guo，BreadZip：a combination of network traffic data and bitmap index encoding algorithm. SMC 2014.

[45] Z. Chen，Y. Wen，W. Zheng，J. Chang，G. Peng，Y. Wu，G. Ma，M. Hakmaoui and J. Cao，A survey of Bitmap Index compression algorithms for Big Data，Tsinghua science and technology，vol. 20，No. 1，2015.

[46] J. Xu，Y. Yu，Z. Chen，B. Cao，W. Dong，Y. Guo and J. Cao. Mobsafe：cloud computing based forensic analysis for massive mobile applications，Tsinghua Science and Technology，vol. 18，no. 4，2013.

后　记

实验室探究课作为国家级精品课程，其主旨是将专业知识大众化，将科研工作的成果以教学探究形式向同学讲授和研讨，一方面可以总结整理科研工作者的研究工作，发现自身的不足和可能的研究方向；另一方面，丰富了学生的知识，开阔了学生的视野，并通过"究"的指导，增强了学生的实践动手的能力和分析研究的能力。

《网络安全原理与技术》实验室探究课自2006年设立以来，经过8年多的反复教学(近140堂课)，已经为清华大学3000多名本科生开设了讲座，选课的同学来自经管、法律、新闻、社会、计算机、环境等全校各个专业。同学们反馈指出该课收益很多，对切身的互联网安全问题有更深的了解。

作者同时承担了计算机系本科生课程《密码学与安全计算》和研究生课程《可信计算平台与可信网络连接》，在授课与课程报告评判中，不断积累和融入最新的成果与见解。

在多年的教学实践中，感受到学生都是富有朝气的一群人，处于人生的关键时期，学业、职业和感情影响很多。学生需要的可能不仅仅是一门课的成绩，特别是对清华大学的学生，有可能还需要自己的老师是一位精神导师，需要从老师这里获得信心和创新的展示机会，以及一段人生成长的指导，一个开放沟通的群体等。那么，一门课程就不仅是一场教学，更像是一个供学生展示成就的小舞台或者小型社交网络，培养锻炼学生全方面的素质与能力。